CANADIAN JOURNAL OF MATHEMATICS

Journal Canadien de Mathématiques

VOL. IV - NO. 1
1952

Published for
THE CANADIAN MATHEMATICAL CONGRESS
by the
University of Toronto Press

The chief languages of the *Journal* are English and French.

Manuscripts for publication in the *Journal* should be sent to the *Editor-in-Chief*, H. S. M. Coxeter, University of Toronto. Every paper should contain an introduction summarizing the results as far as possible in such a way as to be understood by the non-expert.

All other correspondence should be addressed to the *Managing Editor*, G. de B. Robinson, University of Toronto.

The *Journal* is published quarterly. Subscriptions should be sent to the *Managing Editor*. The price per volume of four numbers is $6.00. This is reduced to $3.00 for individual members of the following Societies:

Canadian Mathematical Congress
American Mathematical Society
Mathematical Association of America
London Mathematical Society
Société Mathématique de France

The Canadian Mathematical Congress gratefully acknowledges the assistance of the following towards the cost of publishing this Journal:

University of British Columbia
Ecole Polytechnique
Loyola College
McGill University
Université de Montréal
Royal Military College
Carleton College
Université Laval
University of Manitoba
McMaster University
Queen's University
University of Toronto
National Research Council of Canada
and the
American Mathematical Society

AUTHORIZED AS SECOND CLASS MAIL, POST OFFICE DEPARTMENT, OTTAWA

Foreword to Volume IV

FOR THE past six months the University of Toronto Press has been experimenting with a new method of setting mathematical formulae, with a view to reducing the hand work involved. The reader will notice that in the first five papers in this issue of the *Journal* the indices of the first order are too small while in the remaining papers this fault is corrected and the indices are larger; this change marks a notable improvement in existing practice. It may be of interest to note that only the large brackets and braces and the large integral, product, and summation signs are now inserted by hand; the limits are set in place on the machine. The Editors of the *Journal* are much pleased with the advantages of the new system. The time and cost of setting are both materially reduced and the alignment of first and second order indices is improved. It is hoped to bring out shortly a pamphlet of Instructions to Authors which will explain the new system and offer advice on the preparation of manuscripts.

SUR UN PROBLÈME DE CONFIGURATIONS ET SUR LES FRACTIONS CONTINUES

JACQUES TOUCHARD

Introduction. Dans un précédent article [6, §4] j'ai essayé de traiter le problème suivant, qui fait l'objet du présent travail: on donne $2n$ abscisses, marquées $1, 2, \ldots, 2n$, de gauche à droite, sur un axe horizontal. On les joint deux à deux par n arcs convexes, tracés au-dessus de l'axe, de manière que chaque abscisse soit l'origine ou l'extrémité d'un seul arc, l'origine étant à gauche et l'extrémité à droite. On obtient ainsi $p_{nn} = 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)$ configurations et on demande le nombre de celles qui ont p points doubles.

Je crois devoir rappeler les définitions suivantes. Nous dirons que deux arcs C_1 et C_2 appartiennent à un même système si l'un recouvre l'autre ou si l'un coupe l'autre ou si un troisième arc C_3 recouvre C_1 et C_2 ou les coupe tous les deux, ou encore coupe l'un d'eux et recouvre l'autre. Lorsqu'un système S_1 est recouvert par un arc d'un système S_2 et qu'aucun arc de S_1 n'est coupé par aucun arc de S_2, S_1 et S_2 forment un système S, dont S_1 est un sous-système. Nous dirons qu'un système est propre, lorsqu'il ne contient pas de sous-système.

Ce problème, je l'avais abordé en partant de la notion des systèmes propres, qui sont en effet les éléments en lesquels se décompose toute configuration. Je suis parvenu ainsi à des formules générales, donnant les nombres de configurations qui ont de zéro à six points doubles, mais la difficulté de former les systèmes propres m'avait empêché d'aller plus loin. A la fin de l'article en question, j'ai indiqué le principe d'une autre méthode. Elle consiste à représenter une figure ayant p points doubles par x^p. L'ensemble des configurations de n arcs est ainsi représenté par un polynôme $T_n(x)$, dans lequel le coefficient de x^p est le nombre de celles qui ont p points doubles. De la même manière, les configurations de n arcs, formant un système unique, sont représentées par un polynôme $S_n(x)$ et celles qui forment un système propre par un polynôme $P_n(x)$. C'est la détermination de $S_n(x)$ qui est la plus directe et je l'obtiens aux §§2, 3, 4 en ne faisant, somme toute, que généraliser les propriétés d'un triangle arithmétique, connu sous le nom de triangle de Delannoy et que je rappelle au §1. De même que les nombres de Delannoy peuvent être engendrés par une fraction continue, de même la fonction génératrice des polynômes $S_n(x)$ est une fraction continue $F(x, z)$ que j'étudie aux §§5, 6 et 7. Je détermine ensuite, aux §§8, 9 et 10, les polynômes $T_n(x)$ et $P_n(x)$, ainsi que certaines valeurs numériques. On verra qu'il y a une belle réciprocité entre les polynômes $P_n(x)$ et $S_n(x)$ et on s'explique mal pourquoi la détermination des systèmes propres paraît si difficile, alors que celle des systèmes propres ou impropres est facile. Le §11 contient quelques identités où figurent certaines fonctions d'un usage courant dans la théorie des

Reçu le 22 Novembre, 1950.

fonctions elliptiques. Dans le §12, j'effectue la connexion entre la méthode de mon précédent article [6] et celle employée ici. Cette vérification était nécessaire, car les calculs de mon article [6] reposaient sur la considération de figures assez nombreuses que je n'avais pas reproduites et qui pouvaient prêter à des erreurs. On ne trouvera pas ici l'expression définitive du nombre des configurations ayant un nombre donné de points doubles; on pourrait sans doute y parvenir mais seulement, croyons-nous, au moyen de formules compliquées et peu maniables. La fraction continue $F(x, z)$ est intéressante en elle-même et elle donne, sur le développement de certaines fractions continues, un résultat général qui fait l'objet du §13. Comme la détermination de la valeur de $F(x, z)$ est loin d'être immédiate, j'avais été amené, au cours de divers essais, à former les dérivées partielles d'une fraction continue par rapport à ses éléments. Bien que celles-ci soient très aisées à obtenir, elles ne figurent, à ma connaissance, dans aucun ouvrage. Les formules que je donne au §14 m'ont paru mériter d'être connues. Le §15 contient des tables numériques.

En suivant Perron [3] et pour gagner de la place, j'ai représenté

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \dots}} \qquad \text{par } b_0 + \frac{a_1|}{|b_1} + \frac{a_2|}{|b_2} + \dots$$

et

$$b_0 - \cfrac{a_1}{b_1 - \cfrac{a_2}{b_2 - \dots}} \qquad \text{par } b_0 - \frac{a_1|}{|b_1} - \frac{a_2|}{|b_2} - \dots .$$

1. Le triangle D_p^q de Delannoy [1] est celui-ci

p \ q	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	2			
3	1	3	5	5		
4	1	4	9	14	14	
5	1	5	14	28	42	42

Il est défini par

$$D_p^q = D_{p-1}^q + D_p^{q-1}, \quad D_p^0 = 1. \tag{1}$$

On a

$$D_n^n = D_n^{n-1} = D_{n-1}^0 + D_{n-1}^1 + D_{n-1}^2 + \dots + D_{n-1}^{n-1},$$

$$D_p^q = \frac{p-q+1}{p+1}\binom{p+q}{q},$$

$$D_n^n = D_0^0 D_{n-1}^{n-1} + \dots + D_i^i D_{n-i-1}^{n-i-1} + \dots + D_{n-1}^{n-1} D_0^0. \tag{2}$$

Dans tout cet article, $\phi(z)$ désignera la fonction

$$\phi(z) = \frac{1 - (1 - 4z)^{\frac{1}{2}}}{2z}, \tag{3}$$

$$z\phi^2(z) - \phi(z) + 1 = 0, \tag{4}$$

$$\phi(z) = D_0^1 + D_1^1 z + \ldots + D_n^1 z^n + \ldots, \tag{5}$$

$$[\phi(z)]^{p+1} = D_p^p + D_{p+1}^p z + \ldots + D_{p+n}^p z^n + \ldots, \tag{6}$$

et l'on a, sous forme de fraction continue,

$$\phi(z) = \frac{1}{|1} - \frac{z}{|1} - \frac{z}{|1} - \frac{z}{|1} - \ldots. \tag{7}$$

2. Pour déterminer $S_n(x)$, nous partirons de la remarque suivante. Lorsqu'on a un système de n arcs, $C_1, C_2, \ldots, C_n$, dont les origines respectives, comptées de gauche à droite, sont $\gamma_1, \gamma_2, \ldots, \gamma_n$, si l'on supprime le dernier arc C_n, la figure restante est encore un système. Car, s'il restait deux systèmes, ou bien C_n n'en couperait qu'un et la figure primitive comprendrait deux systèmes, ou bien C_n les couperait tous les deux et alors C_n ne serait pas le dernier arc. Un arc, au moins aurait son origine à droite de γ_n. On peut donc, pour former les systèmes de n arcs, partir des systèmes de $n-1$ arcs, d'origines $\gamma_1, \gamma_2, \ldots, \gamma_{n-1}$ et ajouter un $n$ème arc d'origine γ_n.

Quelles sont les origines des arcs dans un système?

On a évidemment $\gamma_1 = 1$. On a $\gamma_2 = 2$, sans quoi C_1 formerait à lui seul un système. On a $\gamma_3 = 3$ ou 4, car si l'on avait $\gamma_3 \geqslant 5$, C_1 et C_2 formeraient à eux deux au moins un système. En général, $\gamma_k = k, k+1, k+2, \ldots$, ou $2k-2$, car si l'on avait $\gamma_k \geqslant 2k-1$, les arcs $C_1, C_2, \ldots, C_{k-1}$ formeraient à eux seuls au moins un système de $k-1$ arcs et l'ensemble $C_1, C_2, \ldots, C_k, \ldots$ formerait au moins deux systèmes. On peut donc dresser des tableaux, que j'appellerai tableaux Ω_n, pour les origines des arcs d'un système de n arcs.

Ω_1 : 1 .
Ω_2 : 1 2 .
Ω_3 : 1 2 3 , 1 2 4 .
Ω_4 : 1 2 3 4 , 1 2 3 5 , 1 2 3 6 , 1 2 4 5 , 1 2 4 6 .
Ω_5 : 1 2 3 4 5 , 1 2 3 4 6 , 1 2 3 4 7 , 1 2 3 4 8 ,
1 2 3 5 6 , 1 2 3 5 7 , 1 2 3 5 8 , 1 2 3 6 7 , 1 2 3 6 8 ,
1 2 4 5 6 , 1 2 4 5 7 , 1 2 4 5 8 , 1 2 4 6 7 , 1 2 4 6 8 .

Pour former le tableau Ω_{n+1}, on prendra chaque combinaison du tableau Ω_n; soit $\gamma_1 \gamma_2 \ldots \gamma_n$ l'une d'elles; à droite de γ_n on écrira successivement $\gamma_n + 1$, $\gamma_n + 2, \ldots, 2n-1, 2n$.

On peut d'ailleurs former directement le tableau Ω_n par le système d'inégalités

$$\gamma_1 = 1; \gamma_2 = 2; \ldots; k \leqslant \gamma_k \leqslant 2k-2; \ldots; n \leqslant \gamma_n \leqslant 2n-2; \tag{8}$$
$$\gamma_1 < \gamma_2 < \gamma_3 < \ldots < \gamma_n.$$

Voici maintenant la manière d'obtenir les fonctions $S_n(x)$ représentant les configurations de n arcs $C_1, C_2, \ldots, C_n$ ne formant qu'un seul système. Nous l'exposerons en détail pour essayer d'être parfaitement clair. Nous poserons, dans la suite de cette étude, jusqu'au §12 inclusivement,

$$a_p = 1 + x + x^2 + \ldots + x^{p-1}. \tag{9}$$

Pour un seul arc, on a $S_1(x) = 1 = a_1$. Pour deux arcs, $\gamma_2 = 2$; C_2 peut ou non couper C_1, ce qui donne le terme $1 + x = a_2$ et

$$S_2(x) = a_1 a_2.$$

Pour trois arcs, $\gamma_3 = 3$ ou 4. Si $\gamma_3 = 3$, C_3 peut couper 0, 1 ou 2 des arcs C_1 et C_2, ce qui donne le facteur $1 + x + x^2 = a_3$. Si $\gamma_3 = 4$, C_3 peut couper 0 ou 1 arc, ce qui donne le facteur $1 + x = a_2$, de sorte que

$$S_3(x) = a_1 a_2 a_3 + a_1 a_2 a_2.$$

On voit que $S_3(x)$ est formé de deux monômes; dans le premier, la dernière lettre à droite est a_3, ce qui exprime que $\gamma_3 = 3$; dans le second, la dernière lettre à droite est a_2, ce qui exprime que $\gamma_3 = 4$.

Formons encore $S_4(x)$. Si $\gamma_4 = 4$, ce qui ne peut arriver que si $\gamma_3 = 3$, C_4 peut couper 0, 1, 2 ou 3 des arcs C_1, C_2, C_3, ce qui donne le facteur $1 + x + x^2 + x^3 = a_4$, par lequel il faut multiplier le monôme $a_1 a_2 a_3$. Si $\gamma_4 = 5$, ce qui peut arriver si $\gamma_3 = 3$ ou 4, C_4 peut couper 0, 1 ou 2 arcs, ce qui donne le facteur $1 + x + x^2 = a_3$, par lequel il faut multiplier les deux monômes $a_1 a_2 a_3$ et $a_1 a_2 a_2$. Enfin, si $\gamma_4 = 6$, ce qui peut arriver si $\gamma_3 = 3$ ou 4, C_4 peut couper 0 ou 1 arc, ce qui donne le facteur $1 + x = a_2$, par lequel il faut multiplier les deux monômes $a_1 a_2 a_3$ et $a_1 a_2 a_2$. On a donc

$$S_4(x) = a_1 a_2 a_3 a_4 + a_1 a_2 a_3 a_3 + a_1 a_2 a_4 a_3 + a_1 a_2 a_3 a_3 + a_1 a_2 a_2 a_2.$$

Le fait que la dernière lettre à droite d'un monôme est a_4 exprime que $\gamma_4 = 4$; si cette dernière lettre est a_3, c'est que $\gamma_4 = 5$; si elle est a_2, c'est que $\gamma_4 = 6$.

D'une manière générale, $S_n(x)$ se présente sous la forme d'une somme de monômes homogènes en $a_1, a_2, \ldots, a_n$, que nous désignerons par $R_n(a_1, a_2, \ldots, a_n)$ ou, plus brièvement, par $R_n(a)$ et nous supposerons que l'on a pris soin de laisser à la droite de chaque monôme la lettre qui a été écrite la dernière, quand on a formé $R_n(a)$, à partir de $R_{n-1}(a)$.

Formons $S_{n+1}(x) = R_{n+1}(a)$ et, pour cela, considérons un monôme quelconque de $R_n(a)$. Supposons que la dernière lettre à droite soit a_n. Ce fait exprime que $\gamma_n = n$ et alors $\gamma_{n+1} = n + 1, n + 2, \ldots$ ou $2n$. Si $\gamma_{n+1} = n + q$, l'arc C_{n+1} peut couper 0, 1, 2, ... ou $n - q + 1$ des arcs $C_1, C_2, \ldots, C_n$, d'où le facteur

$$1 + x + x^2 + \ldots + x^{n-q+1} = a_{n-q+2}.$$

Ainsi, si $\gamma_n = n$, on devra multiplier le monôme successivement par $a_{n+1}, a_n, a_{n-1}, \ldots, a_2, a_2$. Supposons de même que la dernière lettre à droite soit a_{n-r}; ce fait exprime que $\gamma_n = n + r$ et alors $\gamma_{n+1} = n + r + 1, n + r + 2, \ldots$ ou $2n$, ce qui donne les facteurs $a_{n-r+1}, a_{n-r}, \ldots, a_2, a_2$, par lesquels on devra

multiplier successivement le monôme. Nous avons donc établi les deux règles suivantes:

Première Règle. Pour former $R_{n+1}(a)$ à partir de $R_n(a)$, on considère tous les monômes de $R_n(a)$. Si un monôme se termine à droite par a_i, on le multipliera successivement par $a_{i+1}, a_i, a_{i-1}, \ldots, a_2, a_1$ et on additionnera les résultats.

Deuxième Règle. Il existe une correspondance one-one entre les combinaisons des origines du tableau Ω_n et les monômes de $R_n(a)$. Cette correspondance est la suivante: si la combinaison des origines est $1, 2, \gamma_3, \gamma_4, \ldots, \gamma_n$, les indices des lettres a_i dans le monôme correspondant seront, de gauche à droite,

$$1, 2, 6 - \gamma_3, 8 - \gamma_4, 10 - \gamma_5, \ldots, 2n - \gamma_n.$$

Soit $\gamma'_k = 2k - \gamma_k$ ces indices, $k = 1, 2, \ldots, n$, le système d'inégalités (8) se transforme dans le système

$$\gamma'_1 = 1, \gamma'_2 = 2, \ldots, 2 \leqslant \gamma'_k \leqslant k, \ldots, 2 \leqslant \gamma'_n \leqslant n, \tag{10}$$
$$\gamma'_2 \leqslant \gamma'_3 + 1, \ldots, \gamma'_k \leqslant \gamma'_{k-1} + 1, \ldots, \gamma'_n \leqslant \gamma'_{n-1} + 1,$$

qui permet de former tous les monômes de $R_n(a)$ et, par conséquent, la fonction $R_n(a)$ elle-même. En substituant l'expression (9) de a_p, on aura $S_n(x)$ par des calculs qui se compliquent rapidement.

3. On peut donner à ces calculs plus de régularité de la manière suivante. D'après ce qui précède, $R_n(a)$ est une fonction linéaire des dernières lettres écrites à la droite de chaque monôme. On peut donc poser, pour $n \geqslant 2$

$$R_n(a) = C(n, n)a_n + C(n, n-1)a_{n-1} + \ldots + C(n, i)a_i + \ldots + C(n, 2)a_2. \tag{11}$$

En appliquant la première règle du §2, on trouve

$$C(n+1, n+1) = C(n, n)a_n,$$
$$C(n+1, i) = C(n, n)a_n + C(n, n-1)a_{n-1} + \ldots + C(n, i)a_i + C(n, i-1)a_{i-1} \tag{12}$$

d'où l'on déduit

$$\begin{aligned} C(n+1, n+1) &= C(n, n)a_n \\ C(n+1, n) &= C(n+1, n+1) + C(n, n-1)a_{n-1} \\ &\ldots \qquad\qquad \ldots \\ C(n+1, i) &= C(n+1, i+1) + C(n, i-1)a_{i-1}, \end{aligned} \tag{13}$$

on peut donc former un triangle

$$\begin{array}{l} C(2, 2) \\ C(3, 3)\ C(3, 2) \\ \quad \ldots \\ C(n, n)\ C(n, n-1) \ldots C(n, i) \ldots C(n, 2), \end{array}$$

dont la loi de formation est donnée par (13). D'après (13), on voit que $C(n, 2) = C(n, 3)$ et, en faisant dans (12), $i = 3$ et comparant à (11) on a

$$C(n, 2) = C(n, 3) = R_{n-1}(a). \tag{14}$$

Lorsqu'on fait $x = 0$, on a $a_p = 1$ et l'on retombe sur le triangle de Delannoy, à condition de poser, pour $x = 0$,

$$C(n, n-k) = D^k_{n-k}.$$

A l'aide de la relation (13), on peut former des triangles numériques pour les coefficients de x, x^2, x^3, ... dans les polynômes $C(n, k)$. On trouve ainsi que les trois termes de plus faible degré, dans $S_n(x)$, sont

$$D^{n-1}_{n-1} + (n-1)D^{n-1}_{n-1}x + [\tbinom{n}{2}D^{n-1}_{n-1} - D^{n-2}_n]x^2,$$

mais la loi de formation de ces triangles se complique très vite et je n'ai pas poursuivi dans cette voie.

4. Une expression indépendante des fonctions $C(n+1, r)$ peut s'obtenir de proche, à l'aide de l'équation (13). D'une façon générale, $C(n+1, r)$ s'exprime par une somme multiple d'ordre $n+1-r$, que nous n'écrirons pas, mais nous donnerons, à cause de son importance, l'expression de $C(n+1, 3) = R_n(a)$, par une somme d'ordre $n-2$, savoir

$$R_n(a) = a_1 a_2 \sum_{i_1=2}^{2} \sum_{i_2=2}^{1+i_1} \sum_{i_3=2}^{1+i_2} \cdots \sum_{i_{n-2}=2}^{1+i_{n-3}} a_{i_1} a_{i_2} \cdots a_{i_{n-2}}. \tag{15}$$

C'est précisément l'expression à laquelle conduit le système d'inégalités (10).

5. Il s'agit maintenant de trouver l'analogue de la formule bilinéaire (2), relative aux nombres D^n_n. Or, c'est très facile si on se reporte au tableau Ω_n des origine des arcs et à la deuxième règle du §2. D'après les inégalités (8), il est évident que si l'on considère toutes les combinaisons du tableau Ω_n

$$1\ 2\ \gamma_3\gamma_4 \cdots \gamma_q\gamma_{q+1} \cdots \gamma_n$$

et si on les divise en deux tranches, l'une formée par les q premiers chiffres, l'autre par les $n-q$ suivants, la première tranche comprendra toutes les combinaisons relatives aux q arcs $C_1, C_2, \ldots, C_q$ et la deuxième toutes les combinaisons relatives aux $n-q$ arcs $C_{q+1}, C_{q+2}, \ldots, C_n$. On formera donc le tableau Ω_n en associant:

le tableau pour	C_3	avec le tableau pour	$C_2, C_3 \ldots C_n$,
" "	C_1, C_2	" "	"	$C_3, C_4 \ldots C_n$,
" "	C_1, C_2, C_3	" "	"	$C_4, C_5 \ldots C_n$

et ainsi de suite.

Grâce à la correspondance entre les combinaisons des tableaux Ω_n et les monômes de $R_n(a)$, ceci se traduit par la propriété suivante, qu'il suffit d'exposer sur un exemple, en indiquant par un tiret la division en deux tranches

1 – 2 3 4	$a_1 - a_2\, a_3\, a_4$
1 – 2 3 5	$a_1 - a_2\, a_3\, a_5$
1 2 – 4 5	$a_1\, a_2 - a_3\, a_4$
1 2 3 – 6	$a_1\, a_2\, a_3 - a_4$
1 2 4 – 6	$a_1\, a_2\, a_3 - a_5$

où l'on voit, dans la deuxième colonne, que les groupes de lettres placées à

droite du tiret sont dans leur ensemble les mêmes qu'à gauche du tiret, mais avec des indices augmentés d'une unité. La démonstration est générale et si nous désignons par $R_n(a, 1)$ la fonction $R_n(a)$, dans laquelle tous les indices des a_i ont été augmentés d'une unité, nous aurons

$$(16)\quad R_n(a) = R_1(a)R_{n-1}(a, 1) + R_2(a)R_{n-2}(a, 1) + \ldots + R_{n-1}(a)R_1(a, 1).$$

Posons

$$(17)\quad F(x, z) = R_1(a) + R_2(a)z + \ldots + R_n(a)z^{n-1} + \ldots,$$

et soit $F_1(x, z)$ la fonction F, dans laquelle tous les indices ont été augmentés d'une unité, de sorte que

$$F_1(x, z) = R_1(a, 1) + R_2(a, 1)\, z + \ldots + R_n(a, 1)\, z^{n-1} + \ldots,$$

nous aurons, d'après (16),

$$(18)\qquad zF(x, z)F_1(x, z) - F(x, z) + a_1 = 0.$$

Soit alors $F_k(x, z)$ la fonction $F(x, z)$, où l'on a augmenté tous les indices de k unités, on aura de même

$$(19)\qquad zF_kF_{k+1} - F_k + a_{k+1} = 0$$

et, par suite, sous forme de fraction continue

$$(20)\qquad F(x, z) = \cfrac{a_1}{1} - \cfrac{a_2z}{1} - \cfrac{a_3z}{1} - \cfrac{a_4z}{1} - \ldots,$$

où je rappelle que

$$F(x, z) = S_1(x) + S_2(x)z + \ldots + S_n(x)z^{n-1} + \ldots.$$

Lorsque $|x| < 1$, la série (17) et la fraction continue (20) convergent, [7, p. 45] et [3, p. 258], pour $4|z| < |1 - x|$. Pour $x = 0$, les équations (17), (18), et (20) se réduisent respectivement aux équations (5), (4), et (7), mais on peut aussi généraliser l'équation (6) à l'aide des polynômes $C(p, q)$ du §3. Soit en effet,

$$y_0(z) = C(q, q) + C(q + 1, q)z + \ldots + C(q + n, q)z^n + \ldots.$$

D'après (14), $y_0(z) = F(x, z)$ et l'on trouvera, à l'aide des formules (13) et (19) que $y_0(z) = FF_1F_2 \ldots F_{q-2}$, qui, pour $x = 0$, $q = p + 2$, se réduit au premier membre de l'équation (6).

Voici une autre remarque. D'après la relation (16), $R_n(a, 1)$ s'exprime algébriquement au moyen de $R_2(a), \ldots, R_{n+1}(a)$ et, inversement, $R_n(a)$ s'exprime algébriquement au moyen de $R_1(a, 1), R_2(a, 1) \ldots R_{n-1}(a, 1)$. Or, si l'on forme les fonctions $R_k(a, 1)$, on verra que $R_{n-1}(a, 1)$ représente les configurations de n arcs $C_1, C_2, \ldots C_n$ ne formant qu'un seul système, mais dont les origines, au lieu de satisfaire aux inégalités (8), sont assujetties au système d'inégalités:

$$\gamma_1 = 1, \gamma_2 = 2, \gamma_3 = 3, \ldots, k \leqslant \gamma_k \leqslant 2k - 3, \ldots, n \leqslant \gamma_n \leqslant 2n - 3,$$

$$\gamma_1 < \gamma_2 < \gamma_3 < \ldots < \gamma_n.$$

Il y a donc des relations algébriques entre les fonctions représentant ces systèmes particuliers et celles qui représentent les systèmes les plus généraux.

6. Désignons par

$$\frac{A_1}{B_1} = \frac{a_1}{1}, \quad \frac{A_2}{B_2} = \frac{a_1}{1 - za_2}, \quad \cdots, \frac{A_n}{B_n}, \cdots$$

les réduites de la fraction continue (20), qui sont des fonctions de x et de z. On les obtient à l'aide des formules de récurrence bien connues et le développement en série de Taylor de A_n/B_n coincide avec le développement (17) jusqu'au terme $R_n(a)z^{n-1}$ inclusivement. De plus, lorsque la fraction continue converge, on peut écrire

$$F(x, z) = \frac{A_n}{B_n} + \frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n} + \frac{A_{n+2}}{B_{n+2}} - \frac{A_{n+1}}{B_{n+1}} + \cdots,$$

ou

$$F(x, z) = \frac{A_n}{B_n} + \frac{a_1 a_2 \cdots a_{n+1}}{B_n B_{n+1}} z^n + \frac{a_1 a_2 \cdots a_{n+2}}{B_{n+1} B_{n+2}} z^{n+1} + \cdots. \tag{21}$$

Or, on trouve facilement que

$$\frac{1}{B_n B_{n+1}} = 1 + (2a_2 + 2a_3 + \cdots + 2a_n + a_{n+1})z + z^2\epsilon(z),$$

$\epsilon(z)$ désignant une série entière qui ne s'évanouit pas avec z. En substituant dans (21), on verra que, dans le développement de A_n/B_n, le coefficient de z^n est $R_{n+1}(a) - a_1 a_2 \cdots a_{n+1}$ et que le coefficient de z^{n+1} est

$$R_{n+2}(a) - a_1 a_2 \cdots a_{n+2} - a_1 a_2 \cdots a_{n+1}(2a_2 + 2a_3 + \cdots + 2a_n + a_{n+1}).$$

Supposons maintenant que x soit une racine primitive, $x = \rho_k$, de $a_k = 0$, c'est-à-dire de $x^k - 1 = 0$. On a alors

$$F(\rho_k, z) = A_{k-1}(\rho_k, z)/B_{k-1}(\rho_k, z);$$

$F(\rho_k, z)$ est donc une fraction rationnelle en z qu'il est aisé de former pour $k = 2, 3, 4$. On obtient ainsi des relations qui sont précieuses pour vérifier l'exactitude des coefficients qui figurent dans les polynômes $S_n(x)$. On a $F(-1, z) = 1$, donc $S_n(-1) = 0$, $n \geqslant 2$. Puis, j étant une racine cubique complexe de l'unité, on a

$$F(j, z) = \frac{1 - j^2 z + jz^2}{1 + z^3},$$

donc

$$S_n(j) = (-1)^{n-1} j^{2n-2}, \qquad n \geqslant 1.$$

Enfin, pour $i^2 = -1$,

$$F(i, z) = \frac{1 - iz}{1 - (1 + 2i)z},$$

donc, en développant,

$$S_n(i) = (1+i)(1+2i)^{n-2}, \qquad n \geqslant 2.$$

7. Reste maintenant à trouver la valeur de la fraction continue (20). On obtient une première indication, lorsque, dans (20), on fait $x = 1$ et qu'on remplace z par $-z$. On a alors formellement

$$F(1,-z) = \frac{1|}{|1} + \frac{2z|}{|1} + \frac{3z|}{|1} + \frac{4z|}{|1} + \dots.$$

C'est là un cas particulier de la fraction continue de Gauss. On trouve en effet que

$$(22) \qquad 1 + zF(1,-z) = 1/(1 - z + 1\cdot 3z^2 - 1\cdot 3\cdot 5z^3 + 1\cdot 3\cdot 5\cdot 7z^4 - \dots),$$

formule qui nous servira plus loin. La divergence de la série au dénominateur est ici sans inconvénient; on peut la remplacer par un nombre limité de termes, suivis d'un reste. Si l'on veut,

$$\frac{\pi^{\frac{1}{2}}}{1 + zF(1,-z)} = \int_0^\infty \frac{e^{-u}u^{-\frac{1}{2}}du}{1+2zu}$$

et l'intégrale peut être développée avec un reste. Cela étant, on sait que Heine [2, p. 284] a généralisé la série de Gauss. Il était donc naturel de chercher à utiliser les fractions continues de Heine, mais tout ce que j'ai pu obtenir dans cette voie, c'est une identité intéressante que voici. Soit

$$X(x,z) = 1 + a_1 z + a_1 a_2 z^2 + a_1 a_2 a_3 z^3 + \dots$$

a_n ayant sa signification habituelle (9); on a

$$\frac{1}{X(x,z)} = 1 - \frac{a_1 z|}{|1} - \frac{x a_2 z|}{|1} - \frac{x^2 a_3 z|}{|1} - \frac{x^3 a_4 z|}{|1} - \dots$$

où, sauf un terme constant et un facteur z, on reconnaît la fraction continue (20), dans laquelle on aurait remplacé, pour toute valeur de l'indice i, a_i par $x^{i-1}a_i$. Si on désigne, d'une façon abrégée, par $R_n(x^{i-1}a_i)$ ce que devient alors le polynôme $R_n(a)$, on aura

$$\frac{1}{X(x,z)} = 1 - R_1(x^{i-1}a_i)z - \dots - R_n(x^{i-1}a_i)z^n - \dots$$

d'où l'identité annoncée

$$R_n(x^{i-1}a_i) + a_1 R_{n-1}(x^{i-1}a_i) + a_1 a_2 R_{n-2}(x^{i-1}a_i) + \dots$$
$$+ a_1 a_2 a_3 \dots a_{2n-2} R_1(a_i) = a_1 a_2 a_3 \dots a_{2n-1}.$$

Mais, de cette identité, il ne paraît pas facile de déduire l'expression de la fraction continue (20). J'ai donc cherché à déterminer directement des fonctions $Q_n(x,z)$ par le système d'équations aux différences

$$(23) \qquad Q_{n-1} = Q_n + (1-x^n)zQ_{n+1}, \qquad n = 1, 2, 3, \dots.$$

Il en résultera, d'après un théorème connu [3, p. 291]

$$\frac{Q_0}{Q_1} = 1 + \cfrac{(1-x)z}{1} + \cfrac{(1-x^2)z}{1} + \cfrac{(1-x^3)z}{1} + \dots,$$

c'est-à-dire

$$\frac{Q_0}{Q_1} = 1 + (1-x)zF[x, -(1-x)z]. \tag{24}$$

Je me donne arbitrairement $Q_0 = 1$ et je pose

$$Q_n = f_0(n) + f_1(n)z + \dots + f_p(n)z^p + \dots \tag{25}$$

avec $f_0(n) = 1$.
D'après (23), les fonctions $f_p(n)$ doivent satisfaire aux équations

$$f_p(n) - f_p(n-1) = (x^n - 1)f_{p-1}(n+1). \tag{26}$$

Soit

$$\Phi_n^p(x) = x^{\frac{1}{2}p(p+1)}\frac{(1-x^n)(1-x^{n-1})\dots(1-x^{n-p+1})}{(1-x)(1-x^2)\dots(1-x^p)}$$

avec $\Phi_n^0(x) = 1$; et soit encore

$$E(m,q) = \frac{(m-2q)(m-1)(m-2)\dots(m-q+1)}{q!}, \qquad m > 2q$$

et $E(m,q) = 0$, pour $m \leqslant 2q$ avec $E(m,0) = 1$. Les nombres $E(m,q)$ satisfont aux relations

$$E(m,1) = 1 + E(m-1,1)$$

$$E(m,q) = E(m-1,q-1) + E(m-1,q)$$

et d'autre part, on vérifiera que

$$\Phi_{n+p-1}^p - \Phi_{n+p-2}^{p-1} - \Phi_{n+p-2}^p = (x^n - 1)\Phi_{n+p-1}^{p-1}, \qquad p \geqslant 1. \tag{27}$$

Cela étant, je dis que la fonction

$$f_p(n) = \sum_{i=1}^{p+1} (-1)^{i-1}E(n+2p, i-1)\Phi_{n+p-i}^{p-i+1} \tag{28}$$

satisfait aux équations (26). Pour le voir, il suffira, dans (28), de remplacer $E(n+2p, i-1)$ par $E(n-1+2p, i-2) + E(n-1+2p, i-1)$ puis, après substitution dans le premier membre de (26), de grouper les termes qui ont le même coefficient numérique $E(k,q)$ et de se servir de la formule (27). La fonction (28) est donc une solution de l'équation aux différences (26) et c'est la seule qui convienne, car toute autre solution ne pourrait en différer que par une fonction $\psi_p(n)$, de période 1, par rapport à la variable n, et comme nous avons posé $Q_0 = 1$, il faut, d'après (25) que, sauf pour $p = 0$, nous ayons $f_p(0) = 0$, d'où $\psi_p(n) = \psi_p(0) = 0$.

Faisons maintenant $n = 1$, dans (28), et observons que les nombres $E(m,q)$ ne sont autres que les nombres de Delannoy, dans un autre ordre que dans le triangle du §1, $E(m,i) = D_{m-i-1}^i$, et nous aurons

$$f_0(1) = D^0_0,$$

$$f_1(1) = D^0_1 x - D^1_1,$$

. . . . . .

$$f_p(1) = D^0_{2p} x^{\frac{1}{2}p(p+1)} - D^1_{2p-1} x^{\frac{1}{2}p(p-1)} + D^2_{2p-2} x^{\frac{1}{2}(p-1)(p-2)} - \ldots + (-1)^p D^p_p.$$

Substituons ces valeurs dans la formule (25), en y faisant $n = 1$, ordonnons la série obtenue par rapport aux puissances de x et ayons recours à la formule (6), nous aurons

$$(29) \qquad Q_1 = \phi(-z) + xz\phi^3(-z) + \ldots + x^{\frac{1}{2}p(p+1)} z^p \phi^{2p+1}(-z) + \ldots$$

ou, en posant

$$(30) \qquad A(q, u) = 1 + qu + q^3u^2 + \ldots + q^{\frac{1}{2}p(p+1)}u^p + \ldots$$

$$Q_1 = \phi(-z) A[x, z\phi^2(-z)].$$

On a donc finalement, d'après (24), où $Q_0 = 1$,

$$(31) \qquad 1 + (1-x)zF[x, -(1-x)z] = \frac{1}{\phi(-z)} \frac{1}{A[x, z\phi^2(-z)]}$$

ou bien

$$(32) \qquad 1 - (1-x)zF[x, (1-x)z] = \frac{1 - z\phi(z)}{A[x, 1 - \phi(z)]}.$$

On voit que la fonction $A(q, u)$ se rattache aux fonctions θ de Jacobi, mais ce qui distingue la fraction continue (20) de diverses fractions continues, obtenues autrefois par Heine, Eisenstein [3, p. 315] et Ramanujan [4, p. 215], c'est que dans (30), on a substitué à la variable u une fonction algébrique.

Pour obtenir les fonctions $S_n(x)$, on a, d'après (24) et (25),

$$1 - \sum_1^\infty (-1)^n (1-x)^n S_n(x) = 1 / \sum_0^\infty f_n(1) x^n;$$

on calculera donc les polynômes $f_n(1)$, puis les polynômes

$$g_n(x) = (-1) f_n(1) (1-x)^{-n}$$

et on aura $S_1(x) = g_1(x)$ et, pour $n \geqslant 2$,

$$S_n(x) = g_n(x) - g_{n-1}S_1 - g_{n-2}S_2 - \ldots - g_1 S_{n-1}.$$

Un autre procédé consiste à poser

$$B(q, u) = \{A(q, u)\}^{-1} = 1 + \beta_1(q)u + \ldots + \beta_n(q)u^n + \ldots$$

et il résulte alors de la formule (31), après quelques calculs, que

$$(33) \qquad (1-x)^n S_n(x) = D^{n-1}_{n-1}(1-x) - D^{n-2}_n \beta_2(x) + D^{n-3}_{n+1}\beta_3(x) - D^{n-4}_{n+2}\beta_4(x) + \ldots + (-1)^{n-1} D^0_{2n-2}\beta_n(x).$$

Les polynômes $\beta_n(x)$ sont faciles à calculer. Comme vérification, on doit avoir, pour $n \geqslant 2$, $\beta_n(1) = 0$, $\beta_n(-1) = 2$. Si on les considère comme connus, la

formule (33), après multiplication par $(1-x)^{-n}$, donnera explicitement $S_n(x)$. On trouvera plus loin des tables pour $g_n(x)$, $\beta_n(x)$, $S_n(x)$, et $P_n(x)$.

8. Connaissant $S_n(x)$, nous avons maintenant à déterminer les polynômes $T_n(x)$ qui représentent les configurations totales de n arcs et les polynômes $P_n(x)$, qui représentent les configurations formant un système propre. Pour la brièveté, soit $g(y) = g_0 + g_1 y + \ldots + g_n y^n + \ldots$ une série de Taylor quelconque; nous désignerons par $K(y^n, g)$ le coefficient de y^n dans le développement de g, c'est-à-dire g_n, et nous emploierons aussi un langage abrégé en confondant les configurations avec les fonctions qui les représentent. Cela posé, $T_n(x)$ comprend:

1°, les configurations ne formant qu'un seul système, c'est-à-dire $S_n(x)$; c'est le coefficient $K(z^n, zF)$ de z^n dans $zF(x, z)$.

2°, les configurations formant deux systèmes; c'est $\sum S_p S_q$, $p+q=n$; c'est donc $K(z^n, z^2F^2)$.

3°, les configurations formant trois systèmes; c'est $\sum S_p S_q S_r$, $p+q+r=n$; c'est donc $K(z^n, z^3F^3)$ ... et ainsi de suite. Donc

$$T_n(x) = K(z^n, zF + z^2F^2 + \ldots + z^nF^n)$$

et on peut prolonger la série indéfiniment, puisque $z^{n+1}F^{n+1}$, $z^{n+2}F^{n+2}$, ... ne contiennent pas de terme en z^n. La somme de cette série est

$$\frac{zF}{1-zF} = -1 + \frac{1}{1-zF}$$

donc, en se reportant à la formule (20), $T_n(x)$ est le coefficient de z^n dans le développement de la fraction continue

$$-1 + \cfrac{1}{1} - \cfrac{a_1 z}{1} - \cfrac{a_2 z}{1} - \cfrac{a_3 z}{1} - \ldots.$$

On voit que si, dans la fonction $R_{n+1}(a)$ du §2, on remplace a_1 par 1, a_2 par a_1, a_i par a_{i-1}, on obtient $T_n(x)$, donc

$$T_n(x) = R_{n+1}(1, a_1, a_2, \ldots, a_n), \qquad n \geqslant 1.$$

et on aurait l'expression générale de $T_n(x)$ en modifiant de la même façon la formule (15).

9. Pour avoir $P_n(x)$, nous remarquerons que tout système de n arcs est formé par un système propre, dont un ou plusieurs arcs recouvrent des configurations quelconques, c'est-à-dire des configurations totales; celles-ci prennent place dans les intervalles entre les pieds des arcs du système propre et, s'il s'agit d'un système propre de μ arcs, il y aura $2\mu - 1$ intervalles entre les pieds des arcs. Posons tout de suite

$$\chi(x, z) = \sum_{1}^{\infty} T_n(x) z^n$$

$$\omega(x, z) = \sum_{1}^{\infty} P_n(x) z^n. \tag{34}$$

Nous avons, d'après le §8,

$$\chi(x, z) = \frac{zF(x, z)}{1 - zF(x, z)} \tag{35}$$

et, d'après (17),

$$zF(x, z) = \sum_{1}^{\infty} S_n(x) z^n. \tag{36}$$

Nous ferons $S_0(x) = T_0(x) = P_0(x) = 0$.

La fonction $S_n(x)$ comprend:

1°, les systèmes propres de n arcs, $P_n(x)$;

2°, les systèmes propres de $n - 1$ arcs, $P_{n-1}(x)$. Il y a $\binom{2n-3}{1}$ intervalles où peut prendre place successivement une figure $T_1(x)$, d'où le terme

$$P_{n-1}(x)\binom{2n-3}{1}T_1(x),$$

que nous écrirons $P_{n-1}\binom{2n-3}{1}K(z, \chi)$;

3°, les systèmes propres de $n - 2$ arcs, $P_{n-2}(x)$. Il y a $2n - 5$ intervalles; on peut placer une configuration $T_2(x)$ dans un seul intervalle, d'où le terme $\binom{2n-4}{1}P_{n-2}T_2$; ou bien on peut placer deux configurations $T_1(x)$ dans une combinaison de deux intervalles, d'où le terme $\binom{2n-3}{2}P_{n-2}T_1^2$. On voit que ce sont les partitions du nombre 2, savoir $2 = 2$ et $2 = 1 + 1$, qui se manifestent. L'ensemble des deux termes s'écrit

$$P_{n-2}[\binom{2n-4}{1}K(z^2, \chi) + \binom{2n-3}{2}K(z^2, \chi^2)];$$

4°, les systèmes propres de $n - 3$ arcs, $P_{n-3}(x)$. Il y a $2n - 7$ intervalles, donnant en tout 6 places disponibles pour 3 arcs. Si les 3 arcs sont dans un seul intervalle, ce qui correspond à la partition $3 = 3$, on aura le terme $P_{n-3}\binom{2n-7}{1}T_3$. Si les 3 arcs sont dans deux intervalles, ce qui correspond aux deux partitions, $3 = 1 + 2$ et $3 = 2 + 1$, on aura le terme

$$P_{n-3}\binom{2n-5}{2}(T_1T_2 + T_2T_1).$$

Si les trois arcs sont dans 3 intervalles, ce qui correspond à la partition $3 = 1 + 1 + 1$, on aura le terme $P_{n-3}\binom{2n-6}{3}T_1^3$. L'ensemble des trois termes s'écrit

$$P_{n-3}[\binom{2n-7}{1}K(z^3, \chi) + \binom{2n-5}{2}K(z^2, \chi^2) + \binom{2n-6}{3}K(z^3, \chi^3)];$$

5°, les systèmes formés de $n - 4$ arcs, $P_{n-4}(x)$; la partition $4 = 4$ donne le terme $P_{n-4}\binom{2n-8}{1}T_4$; les partitions $4 = 1 + 3 = 2 + 2 = 3 + 1$ donnent le terme

$$P_{n-4}\binom{n-3}{3}(T_1T_3 + T_2^2 + T_3T_1);$$

les partitions $4 = 1+1+2 = 1+2+1 = 2+1+1$ donnent le terme

$$P_{n-4}\binom{n-3}{3}3T_1^2T_2;$$

la partition $4 = 1+1+1+1$ donne le terme

$$P_{n-4}\binom{n-3}{4}T_1^4.$$

L'ensemble des 4 termes s'écrit

$$P_{n-4}[\binom{n-3}{1}K(z^4, \chi) + \binom{n-3}{2}K(z^4, \chi^2) + \binom{n-3}{2}K(z^4, \chi^2) + \binom{n-3}{4}K(z^4, \chi^4)]$$

et ainsi de suite. On a donc

$$S_n = P_n + P_{n-1}[\binom{n-2}{1}K(z, \chi)] + P_{n-2}[\binom{n-3}{1}K(z^2, \chi) + \binom{n-3}{2}K(z^2, \chi^2)] + \dots.$$

Dans chaque crochet, on peut prolonger la série, car il est clair, par exemple, que $K(z^2, \chi^2)$, $K(z^3, \chi^3)\dots$ sont nuls. De plus, on peut, dans chaque crochet, introduire un terme de la forme $K(z^p, \chi^0) = K(z^p, 1)$, qui est nul, pourvu que $p \geqslant 1$. On a donc

$$S_n = P_n + P_{n-1}K[z, (1+\chi)^{2n-3}] + \dots + P_{n-i}K[z^i, (1+\chi)^{2n-2i-1}] + \dots + P_1K[z^{n-1}, 1+\chi].$$

Le dernier terme est encore exact pour $n = 1$, car il devient $P_1(x)K(1, 1+\chi) = P_1(x)$, ce qui est exact, puisque $S_1(x) = P_1(x)$. Le premier terme P_n peut s'écrire $P_nK[1, (1+\chi)^{2n-1}]$ car $K[1, (1+\chi)^{2n-1}] = 1$ et cette expression est valable pour $n = 1$. Ainsi

$$S_n = P_nK[1, (1+\chi)^{2n-1}] + \dots + P_1K[z^{n-1}, 1+\chi]$$

et cette formule est valable, même pour $n = 0$, puisque $P_0 = T_0 = S_0 = 0$.

Maintenant, il est clair que, quelle que soit $g(z)$,

$$K[z^p, g(z)] = K[z^{p+q}, z^qg(z)];$$

on peut donc écrire

$$S_n = P_nK[z^n, z^n(1+\chi)^{2n-1}] + P_{n-1}K[z^n, z^{n-1}(1+\chi)^{2n-3}] + \dots + P_1K[z^n, z(1+\chi)]$$

et ceci exprime que $S_n(x)$ est le coefficient de z^n dans le développement de

$$P_1z(1+\chi) + P_2z^2(1+\chi)^3 + \dots + P_nz^n(1+\chi)^{2n-1}.$$

On peut prolonger cette série indéfiniment, car, au-delà de $P_nz^n(1+\chi)^{2n-1}$, les termes qui viendront ne contiennent plus z^n. Nous avons donc, d'après (34),

$$\sum_1^\infty S_n(x)z^n = \frac{1}{1+\chi}\omega[x, z(1+\chi)^2],$$

et, d'après (35) et (36),

$$[1 - zF(x, z)]\omega\left[x, \frac{z}{[1 - zF(x, z)]^2}\right] = zF(x, z). \tag{37}$$

Telle est l'équation qui relie la fonction génératrice $\omega(x, z)$ des systèmes propres à la fonction génératrice $zF(x, z)$ des systèmes propres ou impropres.

Définissons une variable u par l'équation

$$z - u[1 - zF(x, z)]^2 = 0, \tag{38}$$

cette équation a une racine $\zeta(x, u)$, que l'on peut développer par la série de Lagrange. D'après les valeurs de $S_n(x)$, données au §15, on a

$$\zeta = u - 2u^2 - (2x - 3)u^3 - (2x^2 + 6x^2 - 6x + 4)u^4 - \dots$$

et il résulte de (37) que

$$\omega(x, u) = \frac{\zeta F(x, \zeta)}{1 - \zeta F(x, \zeta)}. \tag{39}$$

On vérifiera cette formule en faisant $x = 0$. Le seul système propre qui ait zéro point double est représenté par $P_1(x) = 1$, d'où $P_1(0) = 1$, et on doit avoir $\omega(0, u) = u$. Or $F(0, z) = \phi(z)$ et l'équation (38) donne simplement $\zeta = u/(1 + u)^2$. Alors $\zeta F(0, \zeta) = u/(1 + u)$ et, d'après (39), $\omega(0, u) = u$.

On peut donner une forme remarquable aux équations (38) et (39). Posons

$$\psi(x, u) = -uF(x, u) = -\sum_1^\infty S_n(x)u^n. \tag{40}$$

Rappelons aussi que

$$\omega(x, u) = \sum_1^\infty P_n(x)u^n. \tag{41}$$

Alors

$$\left\{\begin{array}{c} \omega(x, u) = -\dfrac{\psi(x, \zeta)}{1 + \psi(x, \zeta)} \\ \text{où } \zeta \text{ est la racine, s'annulant avec } u, \text{ de l'équation} \\ \zeta - u[1 + \psi(x, \zeta)]^2 = 0 \end{array}\right. \tag{42}$$

et inversement

$$\left\{\begin{array}{c} \psi(x, u) = -\dfrac{\omega(x, \zeta)}{1 + \omega(x, \zeta)} \\ \text{où } \zeta \text{ est la racine, s'annulant avec } u, \text{ de l'équation} \\ \zeta - u[1 + \omega(x, \zeta)]^2 = 0. \end{array}\right. \tag{43}$$

La fonction $\psi(x, u)$ se déduit de $\omega(x, u)$ par une certaine opération, que définissent les équations (43) et, inversement, d'après (42), si l'on applique la même opération à la fonction $\psi(x, u)$, on retombe sur $\omega(x, u)$. Les fonctions ψ et ω sont réciproques par rapport à cette opération.

Voici ce qui en résulte pour les polynômes $P_n(x)$ et $S_n(x)$. Considérons une fonction s'annultant avec z

$$C(z) = C_1 z + C_2 z^2 + \ldots + C_n z^n + \ldots$$

la racine, s'annulant avec u, de l'équation

$$\zeta - u[1 + C(\zeta)]^x = 0$$

est, en poussant le calcul jusqu'au terme de degré 5,

$$\zeta = u + 2C_1 u^2 + (5C_1^2 + 2C_2)u^3 + (10C_1^3 + 4C_1^2 + 14C_1C_2 + 2C_3)u^4$$
$$+ (20C_1^4 + 22C_1^2 + 72C_1^2C_2 + 18C_1C_3 + 9C_2^2 + 2C_4)u^5 + \ldots$$

et on trouve ensuite

$$\frac{C(\zeta)}{1 + C(\zeta)} = G_1(C_1)u + G_2(C_1, C_2)u^2 + \ldots + G_n(C_1, C_2, \ldots, C_n)u^n + \ldots,$$

$G_n(C_1, C_2, \ldots, C_n)$ étant un polynôme en $C_1, C_2, \ldots, C_n$.

$$G_1 = C_1$$

$$G_2 = C_1^2 + C_2$$

$$G_3 = 2C_1^3 + 4C_1C_2 + C_3$$

$$G_4 = 10C_1^4 - 5C_1^2 + 15C_1^2C_2 + 6C_1C_3 + 3C_2^2 + C_4$$

$$G_5 = 14C_1^5 + 20C_1^3C_2 + 36C_1^2C_3 + 28C_1^2C_3 + 28C_1C_2^2 + 8C_1C_4 + 8C_2C_3 + C_5.$$

Faisons d'abord $C_n = -S_n(x)$, puis $C_n = P_n(x)$ et reportons-nous aux formules (40) et (41), nous aurons les formules réciproques

$$P_n(x) = -G_n(-S_1, -S_2, \ldots, -S_n),$$

$$S_n(x) = G_n(P_1, P_2, \ldots, P_n),$$

que j'ai vérifiées jusqu'à $n = 4$. La réciprocité serait encore mieux mise en évidence si l'on posait $-S_n(x) = S'_n(x)$.

10. Le nombre des configurations de n arcs qui forment un système unique est $S_n(1)$. On obtient, à l'aide de (22), la récurrence

$$S_n(1) = p_{2n} - p_{2n-2}S_1(1) - p_{2n-4}S_2(1) - p_{2n-6}S_3(1) - \ldots - S_{n-1}(1),$$

où $p_{2n} = 1.3.5.\ldots.(2n-1)$. Le nombre des configurations qui forment un système propre est $P_n(1)$. Il s'agit donc d'avoir $\omega(1, u)$. Au lieu de la formule (39), on emploiera la formule

$$\omega(x, u) = uF(x, \zeta) - u\zeta F'(x, \zeta),$$

qui, d'après (38), lui est équivalente. On a

$$F(1, z) = 1 + 2z + 10z^2 + 74z^3 + 706z^4 + 8162z^5 + 109960z^6 + \ldots;$$

la racine ζ de l'équation (38), pour $x = 1$, est

$$\zeta = u - 2u^2 + u^3 - 6u^4 - 34u^5 - 356u^6 + \ldots,$$

et on a ensuite

$$\omega(1, u) = u + u^2 + 4u^3 + 27u^4 + 248u^5 + 2830u^6 + 37782u^7 + \dots.$$

On calculera beaucoup plus facilement la valeur de $P_n(-1)$, car $F(-1, z) = 1$ et l'équation (38) se réduit à $\zeta - u(1-\zeta)^2 = 0$; la racine qui s'annule avec u est

$$\zeta = \frac{1 + 2u - (1+4u)^{\frac{1}{2}}}{2u};$$

on a ensuite, d'après (39),

$$\omega(-1, u) = u\phi(-u) = D_2^1 u - D_3^1 u^3 + D_4^2 u^4 - \dots,$$

donc $P_n(-1) = (-1)^{n-1} D_{n-1}^{n-1}$. Soit $N_p(n)$ et $N_i(n)$ les nombres des systèmes propres de n arcs, qui ont respectivement un nombre pair et un nombre impair de points doubles, on a

$$N_p(n) - N_i(n) = (-1)^{n-1} D_{n-1}^{n-1},$$

et D_{n-1}^{n-1} est le nombre des configurations de n arcs, sans points doubles.

11. On obtient de la manière suivante des formules qui paraissent intéressantes. Récrivons l'équation (31) ou (32) sous la forme

$$1 - \zeta F(x, \zeta) = \frac{1}{\phi\left(\frac{\zeta}{1-x}\right)} \frac{1}{A\left[x, 1 - \phi\left(\frac{\zeta}{1-x}\right)\right]}. \tag{44}$$

On donnera à ζ une valeur telle que le second membre de (44) prenne une forme simple. On aura une première identité en développant en série le premier membre par la formule (36). Substituons ensuite cette valeur de ζ dans l'équation (38); on en déduira la valeur de u, puis l'expression de $\omega(x, u)$, par la formule (39) ou par la formule plus simple

$$\omega(x, u) = \left(\frac{u}{\zeta}\right)^{\frac{1}{2}} - 1, \tag{45}$$

qui lui est équivalente et où la détermination du radical est celle qui se réduit à $+1$, pour $u = 0$, puisque $\omega(x, 0) = 0$. D'où une deuxième identité en développant le premier membre de (45) par la formule (34). On devra faire bien attention de prendre, pour la fonction algébrique $\phi(z)$, La détermination (3), holomorphe à l'origine et que, à la fin de ce paragraphe, j'appellerai $\phi_1(z)$, et non pas la détermination conjuguée $\phi_2(z)$, infinie à l'origine, seconde racine de l'équation (4). De sorte que, dans l'équation (44), on ne peut pas donner n'importe quelle valeur à

$$\phi\left(\frac{\zeta}{1-x}\right).$$

Soit $\zeta = \frac{1-x}{4}$, d'où $\phi\left(\frac{\zeta}{1-x}\right) = 2$. D'après (44),

$$1 - \frac{1-x}{4} F\left(x, \frac{1-x}{4}\right) = \frac{1}{2\lambda(x)}, \tag{46}$$

où

$$\lambda(x) = 1 - x + x^3 - x^6 + x^{10} - x^{15} + \dots .$$

D'après (38), $u = (1-x)\lambda^2(x)$ et, d'après (45),
$\omega(x, u) = 2\lambda(x) - 1$, d'où les identités

$$\sum_{n=1}^{\infty} S_n(x)\left(\frac{1-x}{4}\right)^n = 1 - \frac{1}{2\lambda(x)}, \tag{47}$$

$$\sum_{n=1}^{\infty} P_n(x)(1-x)^n\lambda^{2n}(x) = 2\lambda(x) - 1. \tag{48}$$

Soit $\zeta = -\frac{x}{1-x}$, $\phi\left(\frac{\zeta}{1-x}\right) = 1 - x$ et soit

$$\mu(x) = 1 + x^2 + x^3 + x^7 + x^{14} + x^{26} + \dots$$

on aura de même

$$\sum_{n=1}^{\infty} (-1)^n S_n(x)\frac{x^n}{(1-x)^n} = 1 - \frac{1}{1-x}\,\frac{1}{\mu(x)}, \tag{49}$$

$$\sum_{n=1}^{\infty} (-1)^n P_n(x)x^n(1-x)^n\mu^{2n}(x) = (1-x)\mu(x) - 1. \tag{50}$$

Dans (38), (44) et (45), changeons x en x^2 et on verra d'une manière analogue qu'en posant

$$\zeta_2 = -x^2/(1-x^2),\ \zeta_3 = -x(1+x)/(1-x),\ \zeta_4 = x(1-x)/(1+x)$$

on a

$$2x^{1/4} + \frac{2x^{9/4}}{1-x^2}\,\frac{1}{1-\zeta_2 F(x^2, \zeta_2)} = \theta_2(0), \tag{51}$$

$$1 + \frac{2x}{1-x}\,\frac{1}{1-\zeta_3 F(x^2, \zeta_3)} = \theta_3(0), \tag{52}$$

$$1 - \frac{2x}{1+x}\,\frac{1}{1-\zeta_4 F(x^2, \zeta_4)} = \theta_4(0), \tag{53}$$

où

$$\theta_2(0) = 2x^{1/4} + 2x^{9/4} + 2x^{25/4} + \dots ,$$

$$\theta_3(0) = 1 + 2x + 2x^4 + 2x^9 + \dots ,$$

$$\theta_4(0) = 1 - 2x + 2x^4 - 2x^9 + \dots ,$$

et l'on aura des formules correspondantes pour $\omega(x^2, u)$. Des formules ci-dessus on tire des fractions continues plus ou moins simples, par exemple

$$2\lambda(x) = \frac{1}{|1} - \frac{|1-x}{|4} - \frac{|1-x^2}{|1} - \frac{|1-x^2}{|4} - \frac{|1-x^4}{|1} - \frac{|1-x^4}{|4} - \dots .$$

Supposons pour simplifier x réel et positif, $0 < x < 1$. La série $F(x, z)$ converge absolument sur tout son cercle de convergence $|z| = \frac{1}{4}(1-x)$. La série $\omega(x, u)$

converge certainement pour $4|u| < 1 - x$, car les systèmes propres ne forment qu'une partie des systèmes propres et impropres et $P_n(x) < S_n(x)$. Je ne suis pas actuellement en mesure d'indiquer quel est le rayon de convergence de $\omega(x, u)$. Sauf pour $x = 0$, ce rayon de convergence est fini, car, à l'aide des formules que j'ai données, dans mon article [6], pour le nombre des systèmes propres de p arcs, ayant $p - 1$ ou p points doubles, on peut démontrer que la série $\omega(x, u)$ est divergente pour $|u| > 4/(27x)$. Il résulte de cela que la série (47) converge pour $0 \leqslant x \leqslant 1$; la série (49) pour $0 \leqslant x \leqslant 3 - 2\sqrt{2} = 0{,}1716$; la série $F(x^3, \zeta_2)$ pour $0 \leqslant x \leqslant \sqrt{2} - 1 = 0{,}4142$; la série $F(x^3, \zeta_3)$ pour $0 \leqslant x \leqslant 3 - 2\sqrt{2}$; la série $F(x^3, \zeta_4)$ pour $0 \leqslant x \leqslant 1$. La série (50) et les séries $\omega(x^3, u)$ correspondant aux valeurs $\zeta_2, \zeta_3, \zeta_4$ convergent pour des valeurs suffisamment petites de x, car les expressions correspondantes de u contiennent x ou x^3 en facteur. Mais la convergence de la série (48) reste actuellement douteuse, car $\lambda(x)$ est supérieure à $\frac{1}{2}$ et la condition $4(1 - x)\,\lambda^2(x) \leqslant 1 - x$ n'est pas remplie.

Considérons maintenant, et en supposant toujours $0 < x < 1$, la fonction $F(x, z)$, prise dans toute sa généralité. D'après (44), c'est une fonction à deux branches, l'une $\Phi_1(x, z)$ donnée par la détermination $\phi_1(z)$ de $\phi(z)$; c'est celle que, jusqu'ici, nous avons constamment appelée $F(x, z)$; l'autre, $\Phi_2(x, z)$ donnée par la détermination $\phi_2(z)$ de $\phi(z)$. On peut définir sans ambiguité $\phi_1(z)$ et $\phi_2(z)$ dans tout le plan z et par suite aussi $\Phi_1(x, z)$ et $\Phi_2(x, z)$, par les équations

$$\frac{1}{1 - z\Phi_1(x, z)} = \phi_1\left(\frac{z}{1 - x}\right) A\left[x, 1 - \phi_1\left(\frac{z}{1 - x}\right)\right],$$

$$\frac{1}{1 - z\Phi_2(x, z)} = \phi_2\left(\frac{z}{1 - x}\right) A\left[x, 1 - \phi_2\left(\frac{z}{1 - x}\right)\right].$$

Or,

$$\phi_1(z)\phi_2(z) = 1/z,\ 1 - \phi_2(z) = 1/[1 - \phi_1(z)]$$

et, d'autre part,

$$A(x, v) + \frac{1}{v} A\left(x, \frac{1}{v}\right) = \sum_{n=0}^{\infty} x^{\frac{1}{2}n(n+1)}(v^n + v^{-n-1}) = \rho(x, v), \tag{54}$$

où

$$\rho(x, v) = (1 + \frac{1}{v}) \prod_{n=1}^{\infty} (1 - x^n)(1 + x^n v)(1 + x^n v^{-1})$$

est une fonction θ proprement dite. Dans (54), faisons $v = 1 - \phi_1\left(\frac{z}{1 - x}\right)$ et multiplions par $\phi_1\left(\frac{z}{1 - x}\right)$ et nous obtiendrons, après un calcul simple,

$$\frac{1}{1 - z\Phi_1(x, z)} - \frac{1}{1 - z\Phi_2(x, z)} = \phi_1\left(\frac{z}{1 - x}\right) \rho\left[x, 1 - \phi_1\left(\frac{z}{1 - x}\right)\right]. \tag{55}$$

C'est la formule que nous voulions établir. Soit alors $1 - \phi_1\left(\frac{z}{1 - x}\right) = -x^p$, on en tire

$$z = \frac{x^p(1-x)}{(1+x^p)^2}, \qquad p = 0, 1, 2, 3, \ldots, \tag{56}$$

et cette expression ne change pas quand on change p en $-p$. Le second membre de (55) s'annule pour toutes ces valeurs de z et s'annule aussi pour $z = \infty$. La fonction générale $F(x, z)$ admet donc non seulement les points doubles $z = \frac{1}{4}(1-x)$ et $z = \infty$, qui sont les points de ramification de $\phi\left(\frac{z}{1-x}\right)$, mais un nombre quelconque fini de points doubles donnés par (56), pour $p = 1, 2, 3, \ldots$ et qui ont $z = 0$ comme point limite, point essentiel de $\Phi_n(x, z)$.

12. Le lecteur est maintenant prié de se reporter à mon article [6]. Les symboles et formules appartenant à cet article seront suivis de l'indication [6]. Je me propose de montrer que l'équation [6, (13)], n'est autre chose que l'équation

$$\omega[x, z[1 + \chi(x, z)]^2] = \chi(x, z) \tag{57}$$

qui se déduit de (37) en éliminant $F(x, z)$, à l'aide de (35).

D'abord $U_{nn}(p)$ est le nombre des configurations de n arcs qui ont p points doubles [6]; c'est donc le coefficient de u^p dans $T_n(u)$, c'est-à-dire le résidu à l'origine, au sens de Cauchy, de $T_n(u)/u^{p+1}$. Il y a exception pour $n = 0$, $p = 0$, car nous avons posé $U_0(0) = 1$, tandis que $T_0(u) = 0$. Donc, d'après [6, (5)], $f_p(x)$ est, pour $p = 0, 1, 2, 3, \ldots$, le résidu à l'origine de

$$[1 + T_1(u)x^2 + T_2(u)x^4 + \ldots]/u^{p+1}:$$

$$f_p(x) = \frac{1}{2\pi i}\int_\gamma \frac{1 + \chi(u, x^2)}{u^{p+1}}\, du,$$

γ étant un petit cercle qui entoure l'origine.

D'après [6, (9)], et en supposant $|z^2| < |u|$, pour être autorisé à sommer, nous avons ensuite

$$y(x, z) = \frac{xz}{2\pi i}\int_\gamma \frac{1 + \chi(u, x^2)}{u - z^2}\, du.$$

Mais la fonction $\chi(u, x^2)$ est holomorphe au voisinage de l'origine et, d'autre part, puisque $|z^2| < |u|$, le cercle γ contient le point z^2. On a donc simplement, d'après l'intégrale de Cauchy,

$$y(x, z) = xz[1 + \chi(z^2, x^2)]. \tag{58}$$

De même, $\sigma_{nn}(p + n - 1)$ est le nombre des systèmes propres de n arcs ayant $p + n - 1$ points doubles [6]; c'est donc le coefficient de u^{p+n-1} dans $P_n(u)$ et, d'après [6, (7)], $g_p(y)$ est le résidu à l'origine de $\omega\left(u, \frac{y^2}{u}\right)/u^p$. Ensuite, d'après [6, (8)], et en supposant $|z^2| < |u|$,

$$G(y, z) = \frac{1}{2\pi i}\int_\gamma u\omega\left(u, \frac{y^2}{u}\right)\frac{du}{u - z^2} \tag{59}$$

Mais il est facile de voir que la fonction $u\omega(u, y^n/u)$ est holomorphe à l'origine. En effet,

$$P_n(u) = \sigma_{nn}(0) + \sigma_{nn}(1)u + \ldots + \sigma_{nn}(p)u^p + \ldots,$$

et il n'existe pas de système propre de n arcs, si $p < n - 1$. Donc le polynôme $P_n(u)$ est divisible par u^{n-1} et

$$u\omega\left(u, \frac{y^n}{u}\right) = P_1(u)y^n + \ldots + \frac{P_n(u)}{u^{n-1}}y^{nn} + \ldots$$

est régulière pour $u = 0$. La formule (59) se réduit donc à

$$G(y, z) = z^n\omega(z^n, y^n/z^n). \tag{60}$$

En portant les expressions (58) et (60) dans l'équation [6, (13)], que je récris

$$zy = xz^n + xG(y, z)$$

et en divisant par xz , on obtient

$$\chi(z^n, x^n) = \omega\{z^n, x^n[1 + \chi(z^n, x^n)]^n\},$$

et il suffit de remplacer z par x^1 et x par z^1 pour obtenir l'équation (57).

Resterait à obtenir les équations algébriques auxquelles satisfont les fonctions $g_p(y)$ ce que nous n'avons pas fait [6]. J'ai remarqué à ce sujet que, d'après [6, (14)] et [6, (15)], les équations satisfaites par $g_0(y)$ et $g_1(y)$ sont les équations de deux cubiques unicursales. On vérifiera en effet que, t désignant un paramètre,

$$\begin{aligned} y &= t - t^3, \\ g_0(y) &= t^3 - t^6, \\ g_1(y) &= -\frac{t^3(t^3 + 1)}{3t^3 - 1}. \end{aligned}$$

13. Si l'on se reporte au §5, on voit que la fraction continue qui figure au second membre de (20) résulte de la relation (16) et celle-ci est une conséquence des deux règles du §2, qui nous ont permis de former les polynômes $R_n(a)$. Ce résultat subsiste évidemment quelle que soit la signification qu'on donne aux lettres $a_1, a_2, a_3, \ldots$. Nous avons donc obtenu, sous forme entièrement explicite et sans avoir recours à la formation de ses réduites, le développement en série

$$\cfrac{a_1z}{\left|1\right.} + \cfrac{a_2z}{\left|1\right.} + \cfrac{a_3z}{\left|1\right.} + \ldots = \sum_{n=1}^{\infty}(-1)^{n-1}R_n(a)z^n$$

d'une fraction continue quelconque du type indiqué. Les polynômes $R_n(a)$ sont donnés par la formule (15). Si on avait à développer la fraction continue

$$G(z) = b_0 + \cfrac{a_1z}{\left|b_1\right.} + \cfrac{a_2z}{\left|b_2\right.} + \ldots,$$

on l'écrirait

$$\frac{G(z)}{b_0} = 1 + \cfrac{a_1z/b_0b_1}{\left|1\right.} + \cfrac{a_2z/b_1b_2}{\left|1\right.} + \cfrac{a_3z/b_2b_3}{\left|1\right.} + \ldots,$$

et l'on aurait

$$G(z)/b_0 = 1 + \sum_{n=1}^{\infty} (-1)^{n-1} R_n(a, b) z^n,$$

où $R_n(a, b)$ désigne la fonction $R_n(a)$ dans laquelle on a remplacé a_i par $a_i/b_{i-1}b_i$ $(i = 1, 2, 3, \ldots)$ et l'on modifierait en conséquence la formule (15).

14. Soit

$$M = b_0 + \frac{a_1|}{|b_1} + \frac{a_2|}{|b_2} + \ldots$$

une fraction continue quelconque et soit $R_k = A_k/B_k$ la $k$ème réduite ou fraction convergente, $R_0 = b_0$, $R_1 = (b_0b_1 + a_1)/b_1, \ldots$. Le symbole R_k n'a plus ici aucun rapport avec la fonction (15) des sections précédentes. En se servant de la formule élémentaire qui donne l'expression de M au moyen d'un quotient complet, en y remplaçant a_k par $a_k + x$, b_k par $b_k + y$ et en développant en série, on trouve

$$(-1)^{(m+n)k} \cdot \frac{(a_1a_2 \ldots a_k)^{m+n}}{(m+n-1)!} \frac{\partial^{m+n} M}{\partial a_k^m \partial b_k^n}$$
$$= (B_{k-2})^{m-1} (B_{k-1})^{n-1} (B_{k-1}M - A_{k-1})^{m+n}$$
$$\cdot [(m+n)B_{k-1}B_{k-2}M - mA_{k-2}B_{k-1} - nA_{k-1}B_{k-2}].$$

En particulier

$$\frac{1}{p!}(R_{k-1} - R_{k-2})^p a_k^p \frac{\partial^p M}{\partial a_k^p} = (M - R_{k-1})^p (M - R_{k-2}), \qquad p \geqslant 1,$$

$$\frac{1}{p!}(R_{k-1} - R_{k-2})^p a_k^p \frac{\partial^p M}{\partial b_k^p} = (B_{k-1})^p (B_{k-2})^{-p} (M - R_{k-1})^{p+1}, \qquad p \geqslant 1.$$

D'autre part, on a aussi

$$M/b_0 = 1 + \frac{a_1/b_0b_1|}{|1} + \frac{a_2/b_1b_2|}{|1} + \frac{a_2/b_2b_3|}{|1} + \ldots$$

et, en considérant (b_0b_1), (b_1b_2), (b_2b_3), ... comme des variables indépendantes, on trouvera par un procédé analogue

$$\frac{(-1)^p}{p!}(R_{k-1} - R_{k-2})^p (b_{k-1}b_k)^p \frac{\partial^p M}{\partial (b_{k-1}b_k)^p}$$
$$= (B_{k-2})^p (M - R_{k-1})(M - R_{k-2})^p.$$

En comparant ces diverses formules, on arrive à des équations aux dérivées partielles qui peuvent, à vrai dire, s'obtenir directement et dont nous ne citerons que celles-ci,

$$a_k \left(\frac{\partial M}{\partial a_k}\right)^2 + \frac{\partial M}{\partial b_{k-1}} \frac{\partial M}{\partial b_k} = 0,$$

$$a_k \frac{\partial M}{\partial a_k} \frac{\partial^2 M}{\partial a_k \partial b_k} = \frac{\partial M}{\partial b_k} \left[\frac{\partial M}{\partial a_k} + a_k \frac{\partial^2 M}{\partial a_k^2}\right].$$

Inversement, certaines relations différentielles, faciles à établir, peuvent conduire, à l'aide des formules ci-dessus, à des identités dont nous citerons la suivante

$$(B_kM - A_k)(B_{k-1}M - A_{k-1}) - a_{k-1}a_k(B_{k-2}M - A_{k-2})(B_{k-2}M - A_{k-2})$$
$$= a_kb_{k-1}(B_{k-2}M - A_{k-2})^2 + b_k(B_{k-1}M - A_{k-1})^2,$$

vérifiée quel que soit M et qui, fort probablement, est déjà connue.

$S_n(x)$

$S_1 = 1$
$S_2 = 1 + x$
$S_3 = 2 + 4x + 3x^2 + x^3$
$S_4 = 5 + 15x + 21x^2 + 18x^3 + 10x^4 + 4x^5 + x^6$
$S_5 = 14 + 56x + 112x^2 + 148x^3 + 143x^4 + 109x^5 + 68x^6 + 35x^7 + 15x^8 + 5x^9 + x^{10}$
$S_6 = 42 + 210x + 540x^2 + 945x^3 + 1255x^4 + 1353x^5 + 1236x^6 + 984x^7 + 696x^8 + 441x^9 + 250x^{10} + 126x^{11} + 56x^{12} + 21x^{13} + 6x^{14} + x^{15}$

$P_n(x)$

$P_1 = 1$
$P_2 = x$
$P_3 = x^3 + 3x^2$
$P_4 = x^6 + 4x^5 + 10x^4 + 12x^3$
$P_5 = x^{10} + 5x^9 + 15x^8 + 35x^7 + 60x^6 + 77x^5 + 55x^4$

$g_n(x)$

$g_1 = 1$
$g_2 = x + 2$
$g_3 = x^3 + 3x^2 + 6x + 5$
$g_4 = x^6 + 4x^5 + 10x^4 + 20x^3 + 28x^2 + 28x + 14$
$g_5 = x^{10} + 5x^9 + 15x^8 + 35x^7 + 70x^6 + 117x^5 + 165x^4 + 195x^3 + 180x^2 + 120x + 42$
$g_6 = x^{15} + 6x^{14} + 21x^{13} + 56x^{12} + 126x^{11} + 252x^{10} + 451x^9 + 726x^8 + 1056x^7 + 1386x^6 + 1617x^5 + 1650x^4 + 1430x^3 + 990x^2 + 495x + 132$

$\beta_n(q)$

$$\beta_1 = -q$$
$$\beta_2 = q^3 - q^2$$
$$\beta_3 = -q^6 + 2q^4 - q^3$$
$$\beta_4 = q^{10} - 3q^8 + q^7 + 2q^6 - q^{10}$$

$$\beta_5 = -q^{15} + 4q^{13} - 3q^{12} - 3q^{11} + 2q^{10} + 2q^{11} - q^{15}$$
$$\beta_6 = q^{21} - 5q^{19} + 6q^{18} + 3q^{17} - 6q^{16} - 2q^{15} + 2q^{14} + 2q^{13} - q^{21}$$
$$\beta_7 = -q^{28} + 6q^{26} - 10q^{25} - q^{24} + 12q^{23} - 3q^{22} + q^{21} - 6q^{20} + 2q^{19} - 3q^{17} + 2q^{16} + 2q^{15} - q^{28}$$
$$\beta_8 = q^{36} - 7q^{34} + 15q^{33} - 4q^{32} - 19q^{31} + 12q^{30} + q^{29} + 9q^{28} - 3q^{27} - 6q^{26} + 4q^{25} - 6q^{24} + q^{23} + 2q^{22} - 3q^{21} + 2q^{20} + 2q^{19} - q^{28}$$

$S_n(1)$

n	1	2	3	4	5	6	7
$S_n(1)$	1	2	10	74	706	8162	109960

$P_n(1)$

n	1	2	3	4	5	6	7
$P_n(1)$	1	1	4	27	248	2830	37782

BIBLIOGRAPHIE

1. A. Errera, *Un problème d'énumération*, Mémoires publiés par l'Académie royale de Belgique, tome 11 (Bruxelles, 1931).
2. E. Heine, *Handbuch der Kugelfunktionen*, 2e éd., tome 1 (Berlin, 1878).
3. O. Perron, *Die Lehre von den Kettenbrüchen*, 2e éd. (Leipzig et Berlin, 1929).
4. S. Ramanujan, *Collected papers* (Cambridge, 1927).
5. J. Touchard, *Sur un problème de configurations*, C. R. de l'Académie des Sciences (Paris), juin 1950.
6. J. Touchard, *Contributions à l'étude du problème des timbres-poste*, Can. J. Math., tome 2 (1950), 385-398.
7. H. S. Wall, *Analytic theory of continued fractions* (New-York, 1948).

Lausanne, Suisse

ZETA FUNCTIONS ON THE UNITARY SPHERE

S. MINAKSHISUNDARAM

1. Introduction. In an earlier paper [5], the author defined a zeta function on the real sphere $x_1^2 + x_2^2 + \ldots + x_{k+1}^2 = 1$, whereas in the present paper it is proposed to define one on the unitary sphere $x_1\bar{x}_1 + x_2\bar{x}_2 + \ldots + x_{k+1}\bar{x}_{k+1} = 1$ where x_i's are complex numbers and $\bar{x}_i$ their complex conjugates. Following E. Cartan, harmonics on the unitary sphere are defined and then a zeta function formed just as in the case of a real sphere. The unitary sphere is seen to behave like an even-dimensional closed manifold, since results similar to the ones proved by the author and A. Pleijel [6] for closed manifolds (of even dimensions) are observed here also.

The zeta function on the real sphere may be viewed as a zeta function associated with the orthogonal group $\mathfrak{O}(n)$ while the one on the unitary sphere as that associated with the unitary group $\mathfrak{U}(n)$. It is clear that one could give a suitable definition of a zeta function on any compact group [8]. If the group acts transitively on a closed manifold with a metric, one could use the idea of harmonics on this manifold [3] and define a zeta function. One could still define harmonics on groups [7] by taking the group itself as the manifold on which the group may act. But in all these cases one should be able to obtain these harmonics as eigenfunctions with associated eigenvalues. That this is possible was shown by Casimir [4]. According to him the elements of the unitary representations of a compact group are the eigenfunctions of a second order differential operator, now known as the Casimir operator. If the eigenvalues of the operator are λ_n with the eigenfunctions ϕ_n, then

$$\Sigma \frac{\phi_n(p)\bar{\phi}_n(q)}{|\lambda_n|^s}$$

will be defined as a zeta function (if the spectrum of the operator is not discrete one will have to use suitable modifications of the definition). Since this series will converge for sufficiently large values of $R(h)$, one may study the analytic continuation of the function so defined.[1] While the discussion of the properties of such functions on abstract groups remains an open question, special cases lend themselves to easy treatment.

Received August 24, 1950. Work completed under contract with the office of Naval Research.

[1] If what Dr. I. Singer has communicated to me is true—that the Casimir operator for a compact Lie group is the Laplace-Beltrami operator—the results that Pleijel and I have proved carry over easily to this case. As pointed out by Hermann Weyl [7] the functional equation, if any, will have to be obtained.

2. Harmonics on the unitary sphere. We enumerate a few properties of harmonics on the unitary sphere $x_1\bar{x}_1 + x_2\bar{x}_2 + \ldots + x_{k+1}\bar{x}_{k+1} = 1$. A full account of them is to be found in Cartan's book on projective geometry [2, chap. V]. Let $V = V(x_1, x_2, \ldots, x_{k+1}, \bar{x}_1, \ldots, \bar{x}_{k+1})$ be an integral polynomial in the $2k + 2$ variables $x_i, \bar{x}_i$, $(i = 1, \ldots, k + 1)$, homogeneous and of degree n in the variables x_i and also homogeneous and of degree n in the variables $\bar{x}_i$. This polynomial is said to be a harmonic of order n, if it satisfies

$$\Delta V \equiv \sum_{i=1}^{k+1} \frac{\partial^2 V}{\partial x_i \partial \bar{x}_i} = 0.$$

There are only a finite number of linearly independent harmonics of order n, their number k_n being given by

$$k_n = k(k + 2n)\left(\frac{(k + 1)(k + 2)\ldots(k + n - 1)}{n!}\right)^2.$$

It is a characteristic property of these polynomials, that any transformation effected on a point of the sphere (leading to another point of the sphere) changes a harmonic of order n to a harmonic of order n which is a linear combination of a basic set of k_n linearly independent harmonics. If we choose the bases to be normal and orthogonal on the sphere and if they are denoted by $U_1^n(M)$, $U_2^n(M)$, $\ldots, U_{k_n}^n(M)$, where M is a point on the sphere, then the expression

$$U_1^n(M)\overline{U}_1^n(M') + \ldots + U_{k_n}^n(M)\overline{U}_{k_n}^n(M'),$$

where M' is another point on the sphere, is invariant for the group of transformations on the unitary sphere, viz., the unitary group. Further, the expression is a function of the geodesic distance between the points. In fact, if r is the geodesic distance, it is a polynomial in $\cos 2r - L_n(\cos 2r)$, say, satisfying the differential equation

$$(1 - z^2)L'' - ((k + 1)z + k - 1)L' + n(n + k)L = 0, \qquad z = \cos 2r.$$

We at once identify a polynomial solution of this equation as the Jacobi polynomial $P_n^{k-1,0}(z)$

$$(1 - z)^{k-1}P_n^{k-1,0}(z) = \frac{(-1)^n}{2^n n!}\frac{d^n}{dz^n}\{(1 - z)^{n+k-1}(1 + z)^n\}.$$

More precisely,

$$\sum_{r=1}^{k_n} U_r^n(M)\overline{U}_r^n(M') = \frac{(2k + n)}{kV}\binom{n+k-1}{n}P_n^{k-1,0}(\cos 2r)$$

$$= \frac{(2k + n)}{kV}P_n^{k-1,0}(1)P_n^{k-1,0}(z),$$

where V is the volume of the sphere and $z = \cos 2r$.

3. Zeta function on the unitary sphere. Inasmuch as we can associate the eigenvalue $n(n+k)$ with any harmonic of order n, we define a zeta function as the analytic continuation of the function represented by the Dirichlet's series

$$(1)\qquad \sum_{n=1}^{\infty} \frac{1}{n^s(n+k)^s} \sum_{r=1}^{h_n} U_r^n(M)U_r^n(M') = \frac{1}{kV} \sum_{n=1}^{\infty} \frac{(2n+k)P_n^{k-1,0}(1)P_n^{k-1,0}(z)}{n^s(n+k)^s}, \qquad s = \sigma + i\tau$$

which has a half-plane of convergence, viz., $R(s) > k$.

We show that *this function is an entire function of s with simple zeros for negative integral values of s provided* $M \neq M'$ *and a meromorphic function of s with simple poles at* $s = 1, 2, \ldots, k$ *if* $M = M'$.

The proof proceeds along the same lines as in our earlier paper [5] and we briefly indicate it here. We need the following [1]

LEMMA.

$$\sum_{n=0}^{\infty} (2n+k)P_n^{k-1,0}(1)P_n^{k-1,0}(\cos 2r)\, t^n = \frac{k(1-t)}{(1+t)^{k+1}} F\left(\frac{k+1}{2}; \frac{k+2}{2}; 1; \frac{\cos^2 r}{\rho^2}\right), \quad \rho = \tfrac{1}{2}(t^{\frac{1}{2}} + t^{-\frac{1}{2}})$$

or

$$(2)\qquad \sum_{n=0}^{\infty} (2n+k)P_n^{k-1,0}(1)P_n^{k-1,0}(\cos 2r)e^{-nt} = \frac{k}{2^k} e^{\frac{1}{2}kt} \frac{\sinh \frac{1}{2}t}{\cosh \frac{1}{2}t} F\left(\frac{k+1}{2}, \frac{k+2}{2}; 1; \frac{\cos^2 r}{\cosh^2 \frac{1}{2}t}\right).$$

From the above lemma we obtain an integral representation of the Dirichlet's series (1) as in [5, (15)].

$$(3)\qquad \sum_{n=1}^{\infty} \frac{(2n+k)P_n^{k-1,0}(1)P_n^{k-1,0}(\cos 2r)}{n^s(n+k)^s} = \left(\frac{4}{k}\right)^{s-1} \frac{\Gamma(s+\frac{1}{2})}{\Gamma(2s)} \int_0^{\infty} \left\{ \frac{k}{2^k} \frac{\sinh \frac{1}{2}t}{(\cosh \frac{1}{2}t)^{k+1}} F\left(\frac{k+1}{2}, \frac{k+2}{2}; 1; \frac{\cos^2 r}{\cosh^2 \frac{1}{2}t}\right) - e^{-\frac{1}{2}kt} \right\} t^{s-\frac{1}{2}} I_{s-\frac{1}{2}}(\tfrac{1}{2}kt)\, dt.$$

If $R(s) > k$, the series on the left converges absolutely and is represented by the integral on the right which converges absolutely if $R(s) > 0$. So the function represented by the series on the left can be continued up to $R(s) = 0$. We shall show, however, that it can be continued over the whole plane adopting the usual procedure of replacing the integral on the right by a contour integral.

In the complex t plane make a cut along the positive side of the real axis from the origin and take a contour C from ∞ in the upper half of the plane, going

round the origin in the anti-clockwise direction and then going back to ∞ in the lower half of the plane (poles of the integrand being in the exterior of C). Now consider the integral along C, viz.,

$$\frac{1}{2\pi i}\int_C \left\{\frac{k}{2^k}\frac{\sinh \tfrac{1}{2}t}{(\cosh \tfrac{1}{2}t)^{k+1}} F\left(\frac{k+1}{2}, \frac{k+2}{2}, 1; \frac{\cos^2 r}{\cosh^2 \tfrac{1}{2}t}\right) - e^{-\frac{1}{2}kt}\right\}$$

(4)

$$(-t)^{s-\frac{1}{2}} I_{s-\frac{1}{2}}(-\tfrac{1}{2}kt)dt = e^{-\pi i(s+\frac{1}{2})}\frac{1}{2\pi i}\int_{-\infty}^{0} + \int + e^{i\pi(s+\frac{1}{2})}\frac{1}{2\pi i}\int_{0}^{\infty}.$$

The second integral on the right, taken along a circle round the origin, is zero since the integrand is regular and hence for $R(s) > 0$, we have

$$\frac{1}{2\pi i}\int_C = \frac{\sin(2s-1)\pi}{\pi}\int_0^\infty.$$

Thus

$$\sum_{n=1}^{\infty} \frac{(2n+k)P_n^{k-1,0}(1)P_n^{k-1,0}(\cos 2r)}{n^s(n+k)^s} = -\left(\frac{4}{k}\right)^{s-\frac{1}{2}} \frac{\Gamma(s+\frac{1}{2})\Gamma(1-2s)}{2\pi i}\int_C \tag{5}$$

for $R(s) > k$. The integral along C is as in (4). Since the contour integral is finite for all values of s, it represents a regular function of s. Thus the series on the left represents an analytic function which can be continued throughout the plane with the possible exception of the simple poles of $\Gamma(1-2s)\Gamma(s+\frac{1}{2})$, viz., half odd integral and positive integral values of s. But the integral is seen to vanish for these values of s, since the integrand is then a regular function of t. To observe that the negative integral values of s are the "trivial" zeros of the function, we have only to note that the residues of the integral are zero. We split the integral as the difference of two, viz.,

$$\int_C \frac{\sinh \tfrac{1}{2}t}{(\cosh \tfrac{1}{2}t)^{k+1}} F\left(\frac{k+1}{2}, \frac{k+2}{2}, 1; \frac{\cos^2 r}{\cosh^2 \tfrac{1}{2}t}\right)(-t)^{s-\frac{1}{2}} I_{s-\frac{1}{2}}(-\tfrac{1}{2}kt)\,dt$$

and

$$\int_C e^{-\frac{1}{2}kt}(-t)^{s-\frac{1}{2}} I_{s-\frac{1}{2}}(-\tfrac{1}{2}kt)\,dt.$$

That the residues are zero in the first case is proved in view of the fact that the integrand is an even function of t for real t, when s is a negative integer. The residues of the second integral are easily calculated to be zero, when s is a negative integer, using the familiar formulas for $e^{-\frac{1}{2}kt}t^{-n-\frac{1}{2}}I_{-n-\frac{1}{2}}(\frac{1}{2}kt)$.

When the two points M and M' coincide, i.e. when $r = 0$, we obtain

$$\sum_{n=1}^{\infty} \frac{(2n+k)\{P_n^{k-1,0}(1)\}^2}{n^s(n+k)^s} = \frac{\Gamma(s+\frac{1}{2})\Gamma(1-2s)}{2\pi i}$$

$$\cdot\int_C \left\{\frac{k}{2^k}\frac{\sinh \tfrac{1}{2}t}{(\cosh \tfrac{1}{2}t)^{k+1}} F\left(\frac{k+1}{2}, \frac{k+2}{2}, 1; \frac{1}{\cosh^2 \tfrac{1}{2}t}\right) - e^{-\frac{1}{2}kt}\right\}(-t)^{s-\frac{1}{2}} I_{s-\frac{1}{2}}(-\tfrac{1}{2}kt)dt.$$

As in the previous case we observe that analytic continuation over the whole plane is possible with the possible exception of the simple poles of $\Gamma(s + \frac{1}{2})$ $\Gamma(1 - 2s)$, viz., half odd integral and positive integral values of s. That part of the integral containing $e^{-\frac{1}{4}kt}$ gives no difficulty, since the integrand is regular for half integral values of s. The first part of the integrand is found to be an even function of t for real t, when s is half an odd integer, taking into account the singularity of the hypergeometric function at $t = 0$. Therefore the residues are zero. Thus half odd integral values do not contribute poles. Further, since we know that the function is regular for $R(s) > k$, we observe that the only poles are $s = 1, 2, \ldots, k$.

References

1. W. N. Bailey, *Generalized hypergeometric series*, Cambridge Tract No. 32 (1935).
2. E. Cartan, *Leçons sur la géométrie projective complexe* (Paris, 1931).
3. ———, *Sur la détermination d'un système orthogonal complet dans un espace de Riemann symétrique clos*, Rend. Circ. Mat. di Palermo, vol. 53 (1929), 217-252.
4. H. B. G. Casimir, *Rotation of a rigid body in quantum mechanics*, Leiden thesis (1931).
5. S. Minakshisundaram, *Zeta function on the sphere*, J. Ind. Math. Soc., vol. 13 (1949), 41-48.
6. S. Minakshisundaram and A. Pleijel, *Some properties of the eigenfunction of the Laplace operator on Riemann manifolds*, Can. J. Math., vol. 1 (1949), 242-286.
7. H. Weyl, *Harmonics on homogeneous manifolds*, Annals of Math., vol. 35 (1934), 485-499.
8. ———, *Ramification, old and new, of the eigenvalue problem*, Bull. Amer. Math. Soc., vol. 56 (1950), 15-139.

Waltair, S. India

THE HOMOMORPHIC MAPPING OF CERTAIN MATRIC ALGEBRAS ONTO RINGS OF DIAGONAL MATRICES

J. K. GOLDHABER

1. Introduction. The problem of determining the conditions under which a finite set of matrices $A_1, A_2, \ldots, A_k$ has the property that their characteristic roots $\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{kj}$ $(j = 1, 2, \ldots, n)$ may be so ordered that every polynomial $f(A_1, A_2, \ldots, A_k)$ in these matrices has characteristic roots $f(\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{kj})$ $(j = 1, 2, \ldots, n)$ was first considered by Frobenius [4]. He showed that a sufficient condition for the $\langle A_i \rangle$ to have this property is that they be commutative. It may be shown by an example that this condition is not necessary.

J. Williamson [9] considered this problem for two matrices under the restriction that one of them be non-derogatory. He then showed that a necessary and sufficient condition that these two matrices have the above property is that they satisfy a certain finite set of matric equations.

N. H. McCoy [7] showed that a necessary and sufficient condition that $A_1, A_2, \ldots, A_k$ have the above property is that $A_rA_s - A_sA_r$ $(r, s = 1, 2, \ldots, k)$ belong to the radical of the algebra generated by the $\langle A_i \rangle$. It may be noted that while on the one hand McCoy's condition removes the restriction that one of the matrices be non-derogatory, it does not, on the other hand, give a criterion, such as the Williamson condition, which may be easily computed.

In a part of the following investigation it is proved that if $\mathfrak{A}$ is a matric algebra such that the sum of every two matrices of $\mathfrak{A}$ has characteristic roots which are the sum of the characteristic roots of the two matrices, then every finite set of matrices of $\mathfrak{A}$ has the above property. This is a small step forward in an attempt to recover the computability of the Williamson condition.

The following mapping theorem, which is used in the proof of the above theorem, is also proved. Let $\mathfrak{A}$ be an algebra over an algebraically closed field $\mathfrak{F}$. Let $\mathfrak{B}$ be an algebra over $\mathfrak{F}$. Let Φ be a mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ which (1) maps the identity of $\mathfrak{A}$, if any, onto the identity of $\mathfrak{B}$, (2) is linear, and (3) maps zero divisors into zero divisors in a strong sense. Then Φ is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ modulo its radical.

Also included in this investigation is a proof of the McCoy condition which is somewhat simpler and more direct than the one originally given by McCoy.

The author wishes to thank the referee for his many helpful suggestions, and in particular for his suggested proofs of Lemma 3.1 and Theorems 4.2 and 5.1.

2. Some known results on the structure of algebras. All the theorems of this section either appear in [1], or are immediate consequences of theorems

Received August 28, 1950.

which appear there. Throughout the discussions of this and subsequent sections $\mathfrak{F}$ shall denote an arbitrary algebraically closed field.

THEOREM 2.1 [1, p. 14]. *If $\mathfrak{D}$ is a division algebra over $\mathfrak{F}$, then $\mathfrak{D} = \mathfrak{F}$.*

THEOREM 2.2 [1, p. 44]. *If $\mathfrak{A}$ is a semi-simple algebra over $\mathfrak{F}$, then $\mathfrak{A}$ is separable over $\mathfrak{F}$.*

THEOREM 2.3 [1, p. 39]. *If $\mathfrak{A}$ is a simple algebra over $\mathfrak{F}$, then $\mathfrak{A}$ is a total matric algebra over $\mathfrak{F}$.*

THEOREM 2.4 [1, p. 39]. *If $\mathfrak{A}$ is a semi-simple algebra over $\mathfrak{F}$, then either $\mathfrak{A}$ is a total matric algebra over $\mathfrak{F}$ or $\mathfrak{A}$ is expressible as the direct sum of total matric algebras over $\mathfrak{F}$.*

THEOREM 2.5. *If $\mathfrak{A}$ is an algebra over $\mathfrak{F}$, then*

$$\mathfrak{A} = (\mathfrak{M}_1 \oplus \mathfrak{M}_2 \oplus \ldots \oplus \mathfrak{M}_k) + \mathfrak{N}$$

where the $\mathfrak{M}_i$ are total matric algebras over $\mathfrak{F}$ and where $\mathfrak{N}$ is the radical of $\mathfrak{A}$. (The symbol $\oplus$ denotes direct sum and the symbol $+$ denotes supplementary sum.)

THEOREM 2.6 [1, p. 40]. *A commutative semi-simple algebra is a direct sum of fields.*

THEOREM 2.7 [1, p. 44]. *Let $\mathfrak{A}$ be an algebra over $\mathfrak{K}$. Then there exists an algebraic extension $\mathfrak{K}'$ of $\mathfrak{K}$ such that $\mathfrak{A}_{\mathfrak{K}'}$ is a diagonal algebra if and only if $\mathfrak{A}$ is a direct sum of separable fields.*

THEOREM 2.8. *If $\mathfrak{A}$ is a commutative semi-simple algebra over an algebraically closed field, then $\mathfrak{A}$ is isomorphic to a diagonal algebra.*

3. Theorems of Frobenius and McCoy.

THEOREM 3.1 [4]. *Let A_i $(i = 1, 2, \ldots, k)$ be a set of commutative matrices. Let $f(x_1, x_2, \ldots, x_k)$ be any polynomial with coefficients in $\mathfrak{F}$. The characteristic roots of A_i, λ_{ij} $(j = 1, 2, \ldots, n)$ may be so ordered that the characteristic roots of $f(A_1, A_2, \ldots, A_k)$ are $f(\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{kj})$. This ordering is the same for every f.*

Every finite set of matrices $\langle A_i \rangle$, commutative or otherwise, which enjoys the property of the preceding theorem will be said to have the *Frobenius Property*.

THEOREM 3.2 [7]. *Let $\langle A_i \rangle_{i=1}^{k}$ be an arbitrary set of matrices all of the same order. Let $\mathfrak{R} = \mathfrak{R}[A_1, A_2, \ldots, A_k]$ denote the algebra of all polynomials in the A_i. Let $\mathfrak{N}$ denote the radical of $\mathfrak{R}$. A necessary and sufficient condition that $\langle A_i \rangle$ have the Frobenius Property is that $A_rA_s - A_sA_r \in \mathfrak{N}$ $(r, s = 1, 2, \ldots, k)$.*

Before proceeding to prove these theorems we shall indicate the mode of approach. If the set of matrices $\langle A_i \rangle$ satisfies the Frobenius condition of commutativity or the McCoy condition (i.e., that $A_rA_s - A_sA_r \in \mathfrak{N}$) then by Theorem 2.8 and Wedderburn's Principal Theorem it follows that the algebra

$\mathfrak{R}[A_1, A_2, \ldots, A_k]$ is homomorphic to a diagonal algebra, the kernel of the homomorphism being the radical of $\mathfrak{R}$. Every diagonal algebra clearly has the Frobenius Property. Therefore, if it is shown that the elements of the radical under the operation of addition do not affect the characteristic roots of the elements of the algebra, then both of the above theorems will follow readily.

LEMMA 3.1. *Let $\mathfrak{A}$ be a matric algebra over $\mathfrak{F}$. Let $\mathfrak{N}$ be the radical of $\mathfrak{A}$. Suppose that the identity matrix $I \in \mathfrak{A}$. If $A \in \mathfrak{A}$ and $N \in \mathfrak{N}$, then A and $A + N$ have the same characteristic function.*

Let z be an indeterminate, and $I = A_0$ the unit matrix. Following [3], define matrices A_k and constants c_k recursively as follows:

$$c_0 = 1,\ c_k = (-1/k)\ \mathrm{tr}(AA_{k-1}),\ A_k = AA_{k-1} + c_kI.$$

Then we have [3]:

$$P(z, A) = \sum_{k=0}^{n-1} A_k z^{n-1-k}, \quad \det(zI - A) = \sum_{k=0}^{n} c_k z^{n-k},$$

where $P(z, A)$ is the adjoint polynomial of $zI - A$.

Now if A is replaced by $A + N$, with N in the radical, the new $(A + N)_k$ differ from the old A_k by elements of the radical, whose trace is zero. Hence the constants c_k are the same for both A and $A + N$, and

$$\det(zI - A) = \det(zI - A - N).$$

LEMMA 3.2. *Let $\mathfrak{A}$ be a semi-simple commutative algebra. Let $\langle A_i \rangle_{i=1}^{k}$ be a set of matrices with $A_i \in \mathfrak{A}$. Then $\langle A_i \rangle_{i=1}^{k}$ has the Frobenius Property.*

By Theorem 2.8 $\mathfrak{A}$ is isomorphic to a diagonal algebra. But clearly any finite set of elements of a diagonal algebra has the Frobenius Property. Hence, because of the existing isomorphism, so does $\langle A_i \rangle_{i=1}^{k}$.

The proof of the sufficiency part of Theorem 3.2, from which Theorem 3.1 follows, may now be given. From Theorem 2.2 and Wedderburn's Principal Theorem it follows that $\mathfrak{N} = \mathfrak{N}' + \mathfrak{N}$ where $\mathfrak{N}' \cong \mathfrak{N} - \mathfrak{N}$. Since $A_rA_s - A_sA_r \in \mathfrak{N}$, it follows that $\mathfrak{N}'$ is a commutative semi-simple algebra. Thus

$$A_i = A_i' + N_i, \qquad A_i' \in \mathfrak{N}', \quad N_i \in \mathfrak{N}.$$

By Lemma 3.1 the characteristic roots of A_i' are the same as those of A_i. By Lemma 3.2 there exists a unique ordering of the roots, λ_{ij}, of the A_i' such that for every polynomial $f(x_1, x_2, \ldots, x_k)$ the characteristic roots of $f(A_1', A_2', \ldots, A_k')$ are $f(\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{kj})$ $(j = 1, 2, \ldots, n)$. Note now that

$$\begin{aligned} f(A_1', A_2', \ldots, A_k') &= f(A_1 - N_1, A_2 - N_2, \ldots, A_k - N_k) \\ &= f(A_1, A_2, \ldots, A_k) + N, \qquad N \in \mathfrak{N}. \end{aligned}$$

Again by Lemma 3.1 the characteristic roots of $f(A_1, A_2, \ldots, A_k)$ are $f(\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{kj})$. Hence the sufficiency of the stated condition has been shown.

The proof of the necessity of the condition of Theorem 3.2 is immediate. For if an ordering of the roots exists then clearly all the roots of

$$f(A_1, A_2, \ldots, A_k) \cdot [A_rA_s - A_sA_r]$$

are zero for every $f(A_1, A_2, \ldots, A_k) \in \mathfrak{R}$ so that $A_rA_s - A_sA_r$ is properly nilpotent in $\mathfrak{R}$ and hence is in $\mathfrak{N}$.

It may be interesting to state Theorem 3.2 in the following equivalent form:

THEOREM 3.2a. *A necessary and sufficient condition that a set of matrices $\langle A_i \rangle_{i=1}^k$ have the Frobenius Property is that there exists a homomorphism of the algebra $\mathfrak{R} = \mathfrak{R}[A_1, A_2, \ldots, A_k]$, with kernel the radical of $\mathfrak{R}$, onto a diagonal algebra.*

4. Concerning characteristic vectors. Rademacher [8] proved Frobenius's Theorem, our Theorem 3.1, by first proving:

THEOREM 4.1. *Let $\langle A_i \rangle_{i=1}^k$ be a set of commutative matrices. Then there exists a set of numbers $\langle \mu_i \rangle_{i=1}^k$ and a row vector ψ, such that*

$$\psi A_i = \mu_i \psi \qquad (i = 1, 2, \ldots, k).$$

A row vector $\psi \neq 0$ which has the property that $\psi A_i = \mu_i \psi$ $(i = 1, 2, \ldots, k)$ is called a *characteristic row vector* associated with the set $\langle A_i \rangle_{i=1}^k$. A characteristic column vector associated with $\langle A_i \rangle_{i=1}^k$ may be defined similarly.

A more general form of the above theorem is given in:

THEOREM 4.2. *Suppose that $A_rA_s - A_sA_r$ $(r, s = 1, 2, \ldots, k)$ is in the radical, $\mathfrak{N}$, of $\mathfrak{R} = \mathfrak{R}[A_1, A_2, \ldots, A_k]$. Let n_c (n_r) denote the nullity of the column (row) space of $\mathfrak{N}$. Then there are exactly n_c (n_r) linearly independent characteristic row (column) vectors associated with $\langle A_i \rangle_{i=1}^k$.*

As above, $\mathfrak{R} = \mathfrak{R}' + \mathfrak{N}$ where $\mathfrak{R}' \cong \mathfrak{R} - \mathfrak{N}$ and where $\mathfrak{R}'$ is a commutative semi-simple algebra. By Theorem 2.8 it may be assumed without loss of generality that $\mathfrak{R}'$ is a diagonal algebra.

Since the nullity of the column space of $\mathfrak{N}$ is n_c, there exists a matrix H of rank n_c such that $HN = 0$, for every $N \in \mathfrak{N}$. Clearly the row vectors of H form a basis for the complement of the column space of $\mathfrak{N}$; that is, if ϕ is a row vector such that $\phi N = 0$ for every $N \in \mathfrak{N}$, then ϕ is a linear combination of the row vectors of H; for otherwise the nullity of the column space of $\mathfrak{N}$ would be greater than n_c.

A matrix is in Hermite form if it is "triangular with zeros above the diagonal; with every diagonal element either zero or one; if the diagonal element in any row is zero, the entire row is zero; if the diagonal element in any column is one, every other element of the column is zero" [6, p. 35].

It may be assumed that H is in Hermite form; for otherwise one may multiply H on the left by a non-singular matrix P which brings H into Hermite form [6, p. 35] and then $(PH)N = H'N = 0$ for every $N \in \mathfrak{N}$. It will be shown that each of the n_c non-zero row vectors of H is a characteristic row vector.

Now $A_i = D_i + N_i$ $(i = 1, 2, \ldots, k)$, where D_i is diagonal and $N_i \in \mathfrak{N}$. Note also that since $D_iN \in \mathfrak{N}$ for every $N \in \mathfrak{N}$ it follows that $(HD_i)N = H(D_iN) = 0$ for every $N \in \mathfrak{N}$; and hence it is true that every row vector of HD_i is a linear combination of the row vectors of H. We may therefore write $HD_i = LH$. If z_i is a number such that the diagonal matrix $B_i = z_iI + D_i$ is non-singular, then

$$HB_i = (z_iI + L)H,$$
$$B_i^{-1}HB_i = B_i^{-1}(z_iI + L)H.$$

The matrix $B_i^{-1}HB_i$ on the left is in Hermite form, since this form is still retained after transforming H by a non-singular diagonal matrix. Since the Hermite form is unique, the right member, which is a left multiple of H, can be in Hermite form only if it is equal to H. Hence B_i and, consequently, D_i are commutative with H. From the equation

$$HA_i = HD_i = D_iH$$

it follows, that if ψ_k is a non-vanishing row vector occupying the kth row of H and λ_{ik} is the kth diagonal element of D_i, then

$$\psi_kA_i = \lambda_{ik}\psi_k.$$

Thus the n_c linearly independent vectors ψ_k are characteristic vectors of each of the matrices A_i.

Suppose now that ψ is any characteristic row vector associated with $\langle A_i \rangle_{i=1}^{k}$; $\psi A_i = \lambda_i\psi$. Let N be any element of $\mathfrak{N}$. Since $N \in \mathfrak{N}[A_1, A_2, \ldots, A_k]$ it is true that $N = f(A_1, A_2, \ldots, A_k)$. Thus

$$\psi N = \psi f(A_1, A_2, \ldots, A_k) = f(\lambda_1, \lambda_2, \ldots, \lambda_k)\psi.$$

But since $N \in \mathfrak{N}$, N has only zero as a characteristic root, and hence $f(\lambda_1, \lambda_2, \ldots, \lambda_k) = 0$. Therefore ψ annihilates every element of $\mathfrak{N}$. But this means that ψ is a linear combination of the n_c vectors ψ_k considered above. This completes the proof of the theorem.

In the example given below $n_c \neq n_r$. This indicates that one cannot in general expect to get an expression for n_c or n_r in terms of the Weyr or Segre characteristics of the matrices involved; for the latter invariants do not differentiate between the structure of the row spaces and the column spaces of the matrices.

Example:
$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$
$$N_1 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad N_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$
$$\mathfrak{N} = \mathfrak{N}[A_1, A_2], \quad \mathfrak{N}' = \mathfrak{N}[I], \quad \mathfrak{N} = \mathfrak{N}[N_1, N_2],$$
$$A_1 = I + N_1, \quad A_2 = I + N_2.$$

Thus $n_e = 1, n_r = 2$. Also note that

$$[1, 0, 0] \cdot A_i = 1 \cdot [1, 0, 0] \qquad (i = 1, 2),$$

$$A_i \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad A_i \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \qquad (i = 1, 2).$$

5. A mapping theorem. $\mathfrak{X}$ is said to be a module over $\mathfrak{F}$ if $\mathfrak{X}$ is a linear subset of an algebra over $\mathfrak{F}$.

Let $\mathfrak{X}$ and $\mathfrak{Y}$ be modules over $\mathfrak{F}$. Let Φ be a mapping of $\mathfrak{X}$ onto $\mathfrak{Y}$ which satisfies the following conditions:

(1) If $\mathfrak{X}$ has a unit ϵ, then $\mathfrak{Y}$ has a unit ϵ', and $\Phi(\epsilon) = \epsilon'$.

C: (2) Φ is linear, i.e., if $X_i \in \mathfrak{X}$ and $a_i \in \mathfrak{F}$, then $\Phi(\sum_{i=1}^{k} a_i X_i) = \sum_{i=1}^{k} a_i \Phi(X_i)$.

(3) If $X_i \in \mathfrak{X}$ and if $\prod_{i=1}^{k} X_i = 0$, then $\prod_{i=1}^{k} \Phi(X_i) = 0$.

THEOREM 5.1. *Let $\mathfrak{M}$ be a total matric algebra over $\mathfrak{F}$, $\mathfrak{Y}$ a module over $\mathfrak{F}$, and Φ a mapping of $\mathfrak{M}$ onto $\mathfrak{Y}$ which satisfies conditions* C. *If $A, A' \in \mathfrak{M}$ then $\Phi(A \cdot A') = \Phi(A)\Phi(A')$. Thus $\mathfrak{Y}$ is an algebra and Φ maps $\mathfrak{M}$ homomorphically onto $\mathfrak{Y}$.*

$\mathfrak{M}$ has a basis E_{ij} $(i, j = 1, 2, \ldots, n)$ where $E_{ij}E_{km} = \delta_{jk}E_{im}$ and where δ_{jk} is Kronecker's delta.

Since Φ is linear it will be sufficient to show that

$$\Phi(E_{ij}E_{km}) = \Phi(E_{ij})\Phi(E_{km}) = \delta_{jk}\Phi(E_{im}).$$

If I is the unit matrix, each of the following products vanishes:

$$E_{ii}E_{km} = 0 \quad \text{for } j \neq k,$$

$$(E_{ii} - I)E_{ik} = E_{ii}E_{ik} - IE_{ik} = 0,$$

$$(E_{ii} - E_{ij})(E_{ik} + E_{jk}) = E_{ii}E_{ik} + E_{ii}E_{jk} - E_{ij}E_{ik} - E_{ij}E_{jk} = 0.$$

Hence the image under the mapping Φ of each of these products vanishes. We obtain successively:

$$\Phi(E_{ij})\Phi(E_{km}) = 0 \quad \text{for } j \neq k,$$

$$\Phi(E_{ii})\Phi(E_{ik}) = \Phi(I)\Phi(E_{ik}) = \Phi(E_{ik}),$$

$$\Phi(E_{ij})\Phi(E_{jk}) = \Phi(E_{ii})\Phi(E_{ik}) + \Phi(E_{ii})\Phi(E_{jk}) - \Phi(E_{ij})\Phi(E_{ik}) = \Phi(E_{ik}).$$

THEOREM 5.2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be algebras over $\mathfrak{F}$ with radicals $\mathfrak{N}$ and $\mathfrak{N}'$ respectively. Let Φ be a mapping of $\mathfrak{A}$ onto $\mathfrak{B}$ which satisfies conditions* C. *If $A, A' \in \mathfrak{A}$ then $\Phi(A \cdot A') = \Phi(A)\Phi(A')$ mod $\mathfrak{N}'$.*

By Theorem 2.5, $\mathfrak{A} = \mathfrak{S} + \mathfrak{N}$ where $\mathfrak{S} = \mathfrak{M}_1 \oplus \mathfrak{M}_2 \oplus \ldots \oplus \mathfrak{M}_k$. Thus if $A \in \mathfrak{A}$ then A is uniquely expressible as $A = S + N$, where $S \in \mathfrak{S}$ and $N \in \mathfrak{N}$.

(1) If $N \in \mathfrak{N}$, then $\Phi(N) \in \mathfrak{N}'$. For suppose that $N \in \mathfrak{N}$. It is sufficient to show that if $B \in \mathfrak{B}$, then $[B\Phi(N)]^l = 0$ for some positive integer l. Since Φ maps $\mathfrak{A}$ *onto* $\mathfrak{B}$ it follows that if $B \in \mathfrak{B}$ there exists an $A \in \mathfrak{A}$ such that $B = \Phi(A)$. Since $N \in \mathfrak{N}$ it is true that there exists an l such that

$$[AN]^l = ANAN \ldots AN = 0.$$

By C_2, $\Phi(A)\Phi(N) \ldots \Phi(A)\Phi(N) = 0$, or $[\Phi(A)\Phi(N)]^l = [B\Phi(N)]^l = 0$. Therefore $\Phi(N) \in \mathfrak{N}'$.

(2) With the use of Theorem 5.1 it may be shown quite easily that if $S, S' \in \mathfrak{S}$, then $\Phi(S)\Phi(S') = \Phi(SS')$.

(3) Suppose now that $A, A' \in \mathfrak{A}$. Then

$$A = S + N, \quad A' = S' + N', \quad S,S' \in \mathfrak{S}, \quad N,N' \in \mathfrak{N},$$
$$AA' = S'' + N'' = (A-N)(A'-N') + N'', \quad S'', (A-N), (A'-N') \in \mathfrak{S}, \quad N'' \in \mathfrak{N}.$$

Using (1) and (2) we may write

$$\Phi(AA') = \Phi(A-N)\Phi(A'-N') + \Phi(N''),$$
$$\Phi(A)\Phi(A') = [\Phi(A-N) + \Phi(N)][\Phi(A'-N') + \Phi(N')],$$
$$\Phi(AA') - \Phi(A)\Phi(A') = \Phi(N'') - \Phi(N)\Phi(A'-N') - \Phi(A-N)\Phi(N') - \Phi(N)\Phi(N') \equiv 0 \mod \mathfrak{N}'.$$

In the preceeding theorem it has been assumed that the field $\mathfrak{F}$ was algebraically closed. The following example shows that Theorem 5.2 is not necessarily true if the field is not algebraically closed. Thus some condition on $\mathfrak{F}$ is necessary. It may be proved that the theorem still holds if the condition of algebraic closure is replaced by the somewhat weaker condition that the characteristic roots of every element of $\mathfrak{A}$ all lie in $\mathfrak{F}$.

Let Ra denote the rational field and let $\mathfrak{A}$ be an algebra over Ra with basis elements I and A, where I is the identity and $A^2 = -I$. Define a mapping Φ of $\mathfrak{A}$ onto $\mathfrak{A}$ as follows:

$$\Phi(aI + bA) = (a + b)I + bA, \qquad a,b \in Ra.$$

Clearly $\Phi(I) = I$; Φ is linear; and since A has no proper zero divisors, Φ satisfies C_2 vacuously. The radical of $\mathfrak{A}$ is zero. Note however that

$$\Phi(A^2) = \Phi(-I) = -I \neq \Phi(A)\Phi(A) = 2A.$$

Note also that if the complex field were used instead of the rational field, and Φ defined similarly, then condition C_2 would not be satisfied. For

$$(iI + A)(iI - A) = 0 \qquad (i^2 = -1),$$

whereas

$$\Phi(iI + A)\Phi(iI - A) = [(i + 1)I + A][(i - 1)I - A] = -I.$$

6. The assignment of a common order to the characteristic roots of certain sets of matrices. Let $\mathfrak{A}$ be a subalgebra of a total matric algebra $\mathfrak{M}$ of order n^2 over an algebraically closed field $\mathfrak{F}$. Suppose that the identity matrix I is in $\mathfrak{A}$. Let λ_{ij} $(j = 1, 2, \ldots, n)$ denote the characteristic roots of $A_i \in \mathfrak{A}$.

$\mathfrak{A}$ is said to have property P_0 if the characteristic roots of every pair of matrices $A_1, A_2 \in \mathfrak{A}$ may be so ordered that the characteristic roots of $A_1 + A_2$ are $\lambda_{1j} + \lambda_{2j}$ $(j = 1, 2, \ldots, n)$.

$\mathfrak{A}$ is said to have property P_1 if the characteristic roots of every finite set of matrices $(A_i)_{i=1}^{k} \in \mathfrak{A}$ may be so ordered that the characteristic roots of $\sum_{i=1}^{k} a_i A_i$ are $\sum_{i=1}^{k} a_i \lambda_{ij}$ $(j = 1, 2, \ldots, n)$ for all $a_i \in \mathfrak{F}$.

The ordering of the roots in property P_0 is not assumed to be unique. It is conceivable, *a priori*, that the jth characteristic root of $A_1 + A_2$ is $\lambda_{1j} + \lambda_{2j}$ but that for some $a \in \mathfrak{F}$ the jth characteristic root of $A_1 + aA_2$ is $\lambda_{1j} + a\lambda_{2k}$; thus it seems possible that the jth root of A_1 may associate with the jth root of A_2 but that for some $a \in \mathfrak{F}$ the jth root of A_1 will associate with the kth root of aA_2. That this is not so is proved in

LEMMA 6.1. *Suppose that $\mathfrak{A}$ has property P_0. Suppose that the jth characteristic root of $A_1 + A_2$ is $\lambda_{1j} + \lambda_{2j}$ $(j = 1, 2, \ldots, n)$. Then the jth characteristic root of $aA_1 + bA_2$ is $a\lambda_{1j} + b\lambda_{2j}$ for all $a, b \in F$ $(j = 1, 2, \ldots, n)$.*

Denote the jth characteristic root of

$$cA_1 + [(a - c)A_1 + bA_2], \quad (a - c)A_1 + bA_2, \text{ and } aA_1 + bA_2$$

by

$$c\lambda_{1j} + (a - c)\lambda_{1l} + b\lambda_{2m}, \quad (a - c)\lambda_{1l} + b\lambda_{2m}, \text{ and } a\lambda_{1p} + b\lambda_{2q}$$

respectively. It would seem that the subscripts l, m, p, and q depend on the values of j, a, b, and c; that is, $l = l(j, a, b, c)$, $m = m(j, a, b, c)$, $p = p(j, a, b, c)$, $q = q(j, a, b, c)$, where the functions involved are integral valued and assume values only between 1 and n inclusive. Since

$$cA_1 + [(a-c)A_1 + bA_2] = aA_1 + bA_2,$$

it is true that

$$c\lambda_{1j} + (a - c)\lambda_{1l(j,a,b,c)} + b\lambda_{2m(j,a,b,c)} = a\lambda_{1p(j,a,b,c)} + b\lambda_{2q(j,a,b,c)}. \tag{6.1}$$

Now let j, b, and c be arbitrary but fixed. Consider the quadruplet of integers $[l(a), m(a), p(a), q(a)]$. Since $l(a)$, $m(a)$, $p(a)$, and $q(a)$ are integers between 1 and n it follows that at most n^4 distinct quadruplets can be obtained by letting a run over $\mathfrak{F}$. Since $\mathfrak{F}$ is algebraically closed it is an infinite field and hence there exist an infinite number of distinct $a_i \in \mathfrak{F}$ such that $[l(a_i), m(a_i), p(a_i), q(a_i)] = [l_0, m_0, p_0, q_0]$ for some fixed l_0, m_0, p_0, and q_0. Thus for an infinite number of distinct $a_i \in \mathfrak{F}$

$$c\lambda_{1j} + (a_i - c)\lambda_{1l_0} + b\lambda_{2m_0} = a\lambda_{1p_0} + b\lambda_{2q_0}. \tag{6.2}$$

From (6.2) it follows immediately that

$$\lambda_{1i_0} = \lambda_{1p_0}. \tag{6.3}$$

Furthermore, $\lambda_{1l(a)}$ *may be taken equal* to λ_{1i_0}, and $\lambda_{1p(a)}$ *may be taken equal* to λ_{1p_0} for all $a \in \mathfrak{F}$. For

$$\begin{aligned}\det(cA_1 + (x-c)A_1 + bA_2 - c\lambda_{1j}I - (x-c)\lambda_{1i_0}I - b\lambda_{2m_0}I)\\ = \det(xA_1 + bA_2 - x\lambda_{1p_0}I - b\lambda_{2q_0}I) = 0\end{aligned}$$

for an infinite number of distinct $x \in \mathfrak{F}$. Hence the above determinants are identically zero, and thus $cA_1 + (a_i - c)A_1 + bA_2$ and $a_iA_1 + bA_2$ have respectively the characteristic roots $c\lambda_{1j} + (a_i - c)\lambda_{1i_0} + b\lambda_{2m_0}$ and $a_i\lambda_{1p_0} + b\lambda_{2q_0}$ for all $a \in \mathfrak{F}$. Consequently one may, without loss of generality, redefine the functions l, m, p, and q so that $[l(a_i), m(a_i), p(a_i), q(a_i)] = [l_0, m_0, p_0, q_0]$ for all $a_i \in \mathfrak{F}$. From this and the fact that the choice of j, b, and c was arbitrary it follows from (6.3) that

$$\lambda_{1l(j,a,b,c)} = \lambda_{1p(j,a,b,c)} \text{ for all } a, b, c \in \mathfrak{F} \qquad (j = 1, 2, \ldots, n).$$

Similarly if j, a, and c are kept fixed it can be shown that

$$\lambda_{2m(j,a,b,c)} = \lambda_{2q(j,a,b,c)} \text{ for all } a, b, c \in \mathfrak{F} \qquad (j = 1, 2, \ldots, n).$$

It has been proved that if the jth root of $(a - c)A_1 + bA_2$ is $(a - c)\lambda_{1l} + b\lambda_{2m}$ then the jth root of $aA_1 + bA_2$ is a $\lambda_{1l} + b\lambda_{2m}$. But the jth root of

$$[a-(a-1)]A_1 + A_2$$

is $\lambda_{1j} + \lambda_{2j}$, and hence the jth root of $aA_1 + A_2$ is $a\lambda_{1j} + \lambda_{2j}$. Applying the same process to $[b - (b-1)]A_1 + aA_2$ one obtains the desired result that the jth root of $aA_1 + bA_2$ is $a\lambda_{1j} + b\lambda_{2j}$ for all $a, b \in \mathfrak{F}$ $(j = 1, 2, \ldots, n)$.

LEMMA 6.2. *Suppose that* $\mathfrak{A}$ *has property* P_0. *Suppose that the jth characteristic root of* $aA_1 + bA_2$ *is* $a\lambda_{1j} + b\lambda_{2j}$ *and that the jth characteristic root of* $aA_2 + bA_2$ *is* $a\lambda_{2j} + b\lambda_{2j}$ *for all* $a, b \in \mathfrak{F}$ $(j = 1, 2, \ldots, n)$. *Then the jth characteristic root of* $aA_1 + bA_2 + cA_2$ *is* $a\lambda_{1j} + b\lambda_{2j} + c\lambda_{2j}$, *for all* $a, b, c \in \mathfrak{F}$.

Note that $aA_1 + bA_2 + cA_2 = [aA_1 + bA_2] + cA_2 = aA_1 + [bA_2 + cA_2]$. Then as in Lemma 6.1, $a\lambda_{1j} + b\lambda_{2j} + c\lambda_{2l(j,a,b,c)} = a\lambda_{1p(m,a,b,c)} + b\lambda_{2m(j,a,b,c)} + c\lambda_{2m(j,a,b,c)}$. Now keep j, a, and b fixed and consider the triplet $[l(c), m(c), p(m, c)]$. Proceeding as in Lemma 6.1, one obtains that $\lambda_{2l(j,a,b,c)} = \lambda_{2m(j,a,b,c)}$ for all $a, b, c \in \mathfrak{F}$ $(j = 1, 2, \ldots, n)$. Similarly keeping j, a, and c fixed gives the result that $\lambda_{2j} = \lambda_{2m(j,a,b,c)}$. From these facts the desired result follows readily.

THEOREM 6.1. *Properties* P_0 *and* P_1 *are equivalent.*

Clearly P_1 implies P_0. The fact that P_0 implies P_1 follows from a simple induction on the number of matrices in Lemma 6.2.

THEOREM 6.2. *Property* P_1 *and the Frobenius Property are equivalent.*

Obviously the Frobenius Property implies property P_1. Suppose that $\mathfrak{A}$ has property P_1. If it is shown that there exists a mapping Φ which

(a) maps $\mathfrak{A}$ onto an algebra $\mathfrak{B}$ which is semi-simple and has the Frobenius Property,

(b) preserves characteristic roots, i.e., A and $\Phi(A)$ have the same characteristic roots, and

(c) satisfies conditions C,

then it will follow from Theorem 5.2 that $\mathfrak{A}$ has the Frobenius Property.

A mapping Φ satisfying these conditions will now be shown to exist.

Let E_i $(i = 1, 2, \ldots, k)$ be a basis for $\mathfrak{A}$. Let ρ_{ij} $(j = 1, 2, \ldots, n)$ denote the characteristic roots of E_i. Define

$$\Phi(E_i) = \begin{bmatrix} \rho_{i1} & 0 & 0 & \ldots & 0 \\ 0 & \rho_{i2} & 0 & \ldots & 0 \\ 0 & 0 & \rho_{i3} & \ldots & 0 \\ & \ldots & & \ldots & \\ 0 & 0 & 0 & \ldots & \rho_{in} \end{bmatrix}$$

where the ρ_{ij} are so ordered that $\Phi(\sum_{i=1}^{k} a_i E_i) = \sum_{i=1}^{k} a_i \Phi(E_i)$ for all $a_i \in \mathfrak{F}$. Since A satisfies P_1 this is possible. Let $\mathfrak{B}$ be the set of all matrices $\langle \Phi(A) \rangle$ with $A \in \mathfrak{A}$.

(a) $\mathfrak{B}$ is a semi-simple algebra with the Frobenius Property.

To prove that $\mathfrak{B}$ is an algebra it will be sufficient to show that if $A_1, A_2 \in \mathfrak{A}$, then there exists an $A_3 \in \mathfrak{A}$ such that $\Phi(A_3) = \Phi(A_1)\Phi(A_2)$, i.e., that $\mathfrak{B}$ is closed under multiplication. Now if $A_1, A_2 \in \mathfrak{A}$, then since $\mathfrak{A}$ has property P_1 it is true that the jth characteristic root of

$$a(A_1 + A_2)^2 + b(A_1 + A_2) + c(A_1^2 + A_2^2)$$

is $a(\lambda_{1j} + \lambda_{2j})^2 + b(\lambda_{1j} + \lambda_{2j}) + c(\lambda_{1j}^2 + \lambda_{2j}^2)$. Letting $a = \frac{1}{2}$, $b = 0$, and $c = -\frac{1}{2}$ one obtains the result that $\Phi(\frac{1}{2}[A_1A_2 + A_2A_1]) = \Phi(A_1)\Phi(A_2)$. Thus $\mathfrak{B}$ is an algebra. Furthermore, since $\mathfrak{B}$ consists of diagonal matrices only, it is semi-simple and has the Frobenius Property.

(b) Φ, by construction, preserves characteristic roots.

(c) Φ satisfies conditions C.

(1) $I \in \mathfrak{A}$ and $\Phi(I) = I$, so that Φ satisfies C_1.

(2) Φ, by construction is linear. Hence Φ satisfies C_2.

(3) It is required to show that if $\prod_{i=1}^{h} A_i = 0$, then $\prod_{i=1}^{h} \Phi(A_i) = 0$; by the

construction of Φ it is thus required to prove that if $\prod_{i=1}^{h} A_i = 0$, then $\prod_{i=1}^{h} \lambda_{ij} = 0$ $(j = 1, 2, \ldots, n)$, where the λ_{ij} are so ordered that $\sum_{i=1}^{h} a_i A_i$ has characteristic roots $\sum_{i=1}^{h} a_i \lambda_{ij}$. This shall be proved by an induction on h.

Let $h = 2$ and suppose that $A_1 A_2 = 0$. Consider $A_2 A_1 = N$. N is nilpotent; for $N^2 = 0$. Furthermore, if $f(A_1, A_2) \in \mathfrak{R}[A_1, A_2]$ then since $A_1 A_2 = 0$, $f(A_1, A_2) \cdot [A_2 A_1] = \sum_i a_i A_2^{r_i} A_1$, where $r_i > 0$ for all i. But $(\sum_i a_i A_2^{r_i} A_1)^2 = 0$. Therefore $N = A_2 A_1$ is the radical of $\mathfrak{R}[A_1, A_2]$. Then $A_2 A_1 - A_1 A_2 = N$ is in the radical of $\mathfrak{R}[A_1, A_2]$ and by Theorem 3.2, $\lambda_{1j}\lambda_{2j} = 0$ $(j = 1, 2, \ldots, n)$, where the λ_{ij} are so ordered that the characteristic roots of $a_1 A_1 + a_2 A_2$ are $a_1\lambda_{1j} + a_2\lambda_{2j}$ for all $a_1, a_2 \in \mathfrak{F}$.

Assume now that if $\prod_{i=1}^{h} A_i = 0$, then $\prod_{i=1}^{h} \lambda_{ij} = 0$ $(j = 1, 2, \ldots, n)$. Suppose that $\prod_{i=1}^{h+1} A_i = 0$. Then $(A_1 A_2) \prod_{i=3}^{h+1} A_i = 0$. By the induction assumption $\mu_j \prod_{i=3}^{h+1} \lambda_{ij} = 0$ where μ_j is the characteristic root of $A_1 A_2$ associated with λ_{ij} $(i = 1, 2, \ldots, h+1)$. Suppose that for some j, $\prod_{i=3}^{h+1} \lambda_{ij} \neq 0$. Then $\mu_j = 0$. It must be shown that either λ_{1j} or λ_{2j} (or both) equals zero.

Consider the matrix

$$B_a = A_1 A_2 - a/(a-1) \cdot \lambda_{2j} A_1 - a\lambda_{1j} A_2 + a^2/(a-1) \cdot \lambda_{1j}\lambda_{2j} I$$
$$= [A_1 - a\lambda_{1j} I][A_2 - a/(a-1) \cdot \lambda_{2j} I], \qquad a \neq 1.$$

Since $\mu_j = 0$ and since $\mathfrak{A}$ has property P_1, B_a has for each $a \in \mathfrak{F}$, $a \neq 1$, a characteristic root equal to zero. Thus for every $a \neq 1$ there exists a vector $\phi_a \neq 0$ such that $B_a \phi_a = 0$. Thus

$$[A_1 - a\lambda_{1j} I][A_2 - a/(a-1) \cdot \lambda_{2j} I]\phi_a = 0.$$

Let $[A_2 - a/(a-1) \cdot \lambda_{2j} I]\phi_a = \psi_a$. Now clearly if $\psi_a \neq 0$, then

$$[A_1 - a\lambda_{1j} I]\,\psi_a = 0.$$

Thus either $[A_2 - a/(a-1) \cdot \lambda_{2j} I]\phi_a = 0$, $\phi_a \neq 0$ for an infinite number of distinct $a \in \mathfrak{F}$, or $[A_1 - a\lambda_{1j} I]\psi_a = 0$, $\psi_a \neq 0$ for an infinite number of distinct $a \in \mathfrak{F}$ (or both). Suppose, say, that $[A_2 - a/(a-1) \cdot \lambda_{2j} I]\phi_a = 0$, $\phi_a \neq 0$ for an infinite number of distinct $a \in \mathfrak{F}$. Then A_2 has characteristic roots $a/(a-1) \cdot \lambda_{2j}$ for an infinite number of distinct $a \in \mathfrak{F}$. But A_2 has only a finite number of distinct characteristic roots. Therefore, for some $a_1, a_2, a_3 \neq a_2$ it is true that $a_1/(a_1 - 1) \cdot \lambda_{2j} = a_3/(a_3 - 1) \cdot \lambda_{2j}$. From this it follows that $\lambda_{2j} = 0$.

By induction it follows that Φ satisfies C_2. Hence the theorem.

As a corollary to the two preceeding theorems we have:

THEOREM 6.3. P_0, P_1, *and the Frobenius Property are equivalent.*

REFERENCES

1. A. A. Albert, *Structure of Algebras* (New York, 1946).
2. H. E. Fettis, *A method for obtaining the characteristic equation of a matrix and computing the associated modal columns*, Quarterly J. Appl. Math., vol 8 (1950), 206-212.
3. J. S. Frame, *A simple recursion formula for inverting a matrix*, Abstract 471, Bull. Amer. Math. Soc., vol. 55 (1949), 1045.
4. G. Frobenius, *Über vertauschbare Matrizen*, Sitz. preuss. Akad. Wiss. (1896), 601-614.
5. C. C. MacDuffee, *The theory of matrices*, Ergeb. der Math., vol. 2 (1933).
6. ———, *Vectors and matrices*, Carus Mathematical Monograph no. 7 (1943).
7. N. H. McCoy, *On the characteristic roots of matric polynomials*, Bull. Amer. Math. Soc., vol. 42 (1936), 592-600.
8. H. Rademacher, *On a theorem of Frobenius*, Studies and Essays presented to R. Courant (New York, 1948), 301-305.
9. J. Williamson, *The simultaneous reduction of two matrices to triangular form*, Amer. J. Math., vol. 57 (1935), 281-293.

University of Wisconsin

CONTRIBUTIONS TO NONCOMMUTATIVE IDEAL THEORY

D. C. MURDOCH

Introduction. The well-known results of Krull concerning the minimal prime divisors and the radical of an ideal in a commutative ring have been extended to the noncommutative case in a recent paper [5] by N. H. McCoy. In that paper systematic use was made of the concept of an m-system, a set M of elements of the ring such that if $a \in M$ and $b \in M$ then $axb \in M$ for some element x of the ring. The m-system plays the same role in the noncommutative case that the multiplicatively closed system plays in the theory of Krull. For example, an ideal in a noncommutative ring is prime if and only if its complement is an m-system. What follows is an attempt based on the methods of McCoy to extend more of the Krull-Noether theory of commutative rings to the noncommutative case. Different treatments of the noncommutative case have previously been published by Krull [2], and Fitting [1]. Since the point of view of the present paper, however, is considerably different from that of either of these previous ones, little or no use has been made of their results. The results and methods of McCoy [5], on the other hand, have been used extensively.

The concept of an isolated component ideal (Krull [3] and [4]) leads in the noncommutative case to upper and lower right (or left) isolated component ideals each of which retains some of the properties of the isolated component ideals of the commutative case. These upper and lower components and the relations between them are investigated in §§ 2, 3 and 4. The results of these sections follow without any assumptions of finite chain conditions. The effect of descending and ascending chain conditions is considered in §5 and the latter is assumed in the remainder of the paper. Right primary ideals are defined in a manner which ensures, in the presence of either chain condition, that the radical of a right primary ideal is prime. The term *radical* is used throughout in the sense of McCoy [5]. Examples are given which show that not every ideal is representable as the intersection of a finite number of right primary ideals but any ideal which is so representable has a short representation and for short representations the same uniqueness theorems hold as in the commutative case. Thus in any two short representations of an ideal $\mathfrak{o}$ as the intersection of right primary ideals the number of primary components is the same and the radicals of these coincide in some order. Moreover, the isolated primary components are uniquely determined and must occur in any such representation of $\mathfrak{o}$.

1. Definitions and basic concepts. Let R be an arbitrary noncommutative ring. An ideal $\mathfrak{p}$ in R is prime if $\mathfrak{ab} \subseteq \mathfrak{p}$ implies either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$, where $\mathfrak{a}$

Received September 22, 1950.

and $\mathfrak{b}$ are any ideals of R. It has been shown by McCoy [5] that an ideal $\mathfrak{p}$ is prime if and only if, for any elements a, b of R, $aRb \subseteq \mathfrak{p}$ implies that either a or b belongs to $\mathfrak{p}$.

DEFINITION 1.1. *A set M of elements of R is called an m-system if for any two elements a and b of M, there exists an element x of R such that $axb \in M$. The null set is also defined to be an m-system* (McCoy [5]).

It is clear from the above remark and from the definition that an ideal is prime if and only if its complement in R is an m-system.

DEFINITION 1.2. *An element a of R is said to be right prime to an ideal $\mathfrak{a}$ if $xRa \subseteq \mathfrak{a}$ implies that $x \in \mathfrak{a}$. An ideal $\mathfrak{b}$ is right prime to $\mathfrak{a}$ if it contains an element which is right prime to $\mathfrak{a}$.*

Elements and ideals left prime to $\mathfrak{a}$ can be defined in the obvious way but the left hand definitions and theorems will usually be omitted.

DEFINITION 1.3. *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in R, the ideal consisting of all elements x of R such that $xRb \subseteq \mathfrak{a}$ for all b in $\mathfrak{b}$ is called the right ideal quotient of $\mathfrak{a}$ by $\mathfrak{b}$ and is denoted by $\mathfrak{a}\mathfrak{b}^{-1}$. Similarly $\mathfrak{b}^{-1}\mathfrak{a}$ consists of all x in R such that $bRx \subseteq \mathfrak{a}$ for all b in $\mathfrak{b}$.*

It is obvious that $\mathfrak{a}\mathfrak{b}^{-1}$ and $\mathfrak{b}^{-1}\mathfrak{a}$ always contain $\mathfrak{a}$ and that if $\mathfrak{b}$ is right prime to $\mathfrak{a}$ then $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}$.

DEFINITION 1.4. *If M is a non-null m-system, a set N of elements of R is called a right n-system associated with M (briefly a right M-n-system) if N contains M and if for every m in M and every n in N there exists an element x of R such that $nxm \in N$. If M is the null set the only right M-n-system is, by definition, the null set itself.*

We note that every m-system is a right (or left) n-system associated with itself. Moreover, the set-theoretic union of a finite or infinite number of right n-systems all of which are associated with the same m-system M, is again a right n-system associated with M. However it may also be associated with a larger m-system, properly containing M. As an illustration of this let R be the ring of integers, p any prime, and M the m-system consisting of all integers prime to p. Let N_i be the set of all integers which are not divisible by p^i ($i = 2, 3, 4, \ldots$). Each N_i is an M-n-system. The union of all N_i is the set of all non-zero integers and is itself an m-system $\bar{M}$. It is therefore an $\bar{M}$-n-system where $\bar{M} \supset M$. We remark also that if, in a commutative ring, $\mathfrak{q}$ is a primary ideal and $\mathfrak{p}$ its associated prime, then $M = C(\mathfrak{p})$ (complement of $\mathfrak{p}$ in R) is an m-system and $N = C(\mathfrak{q})$ is an M-n-system.

2. Upper isolated component ideals.

DEFINITION 2.1. *If $\mathfrak{a}$ is any ideal in R and M is an m-system which does not meet $\mathfrak{a}$ (i.e. has no elements in common with $\mathfrak{a}$), the right upper M-component of $\mathfrak{a}$ is defined to be the set of all elements x of R having the property that every right M-n-system which contains x meets $\mathfrak{a}$.*

The right upper M-component of $\mathfrak{a}$ will be denoted by $\mathfrak{u}(\mathfrak{a}, M)$. In order to show that $\mathfrak{u}(\mathfrak{a}, M)$ is an ideal we shall require the following lemmas.

LEMMA 1. *If $\mathfrak{a}$ is any ideal and M an m-system which does not meet $\mathfrak{a}$ then there exists a maximal right M-n-system N which does not meet $\mathfrak{a}$ and N is uniquely determined by M and $\mathfrak{a}$.*

Proof. There exists at least one right M-n-system which does not meet $\mathfrak{a}$, namely M itself. The union N of all such right M-n-systems therefore satisfies the requirements of the lemma.

LEMMA 2. *Let M be any m-system and N any right M-n-system. Let $\mathfrak{a}$ be an ideal which does not meet N. Then $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{q}^*$ which does not meet N and $\mathfrak{q}^*$ has the property that if $aRb \subseteq \mathfrak{q}^*$ and $b \in M$, then $a \in \mathfrak{q}^*$.*

Proof. Since the union of any linearly ordered set of ideals which do not meet N is an ideal which does not meet N, the existence of $\mathfrak{q}^*$ follows from Zorn's Lemma [6, p. 101].

Now suppose a is an element of R which does not belong to $\mathfrak{q}^*$. Then $(a, \mathfrak{q}^*)$ properly contains $\mathfrak{q}^*$ and hence by the maximal property of $\mathfrak{q}^*$ must contain an element n of N. Thus

$$n = ia + ra + ar' + \sum_{i,l} r_i a r_l + q$$

where i is an integer, r, r', r_i, r_l are elements of R and $q \in \mathfrak{q}^*$. Now if $b \in M$ there exists an element x of R such that $nxb \in N$ where

$$nxb = iaxb + raxb + ar'xb + \sum_{i,l} r_i a r_l xb + qxb.$$

But if $aRb \subseteq \mathfrak{q}^*$ every element in the sum on the right hand side of this equation belongs to $\mathfrak{q}^*$, and nxb belongs to both N and $\mathfrak{q}^*$, contrary to the definition of $\mathfrak{q}^*$. Hence if $aRb \subseteq \mathfrak{q}^*$ and $b \in M$ we must have $a \in \mathfrak{q}^*$, as required.

Lemma 2 states that every element of M is right prime to $\mathfrak{q}^*$. It will be convenient to refer to this property by saying that $\mathfrak{q}^*$ has property (A) relative to M. We remark also that if an ideal has property (A) relative to M then its complement in R is a right M-n-system and conversely.

LEMMA 3. *Let $\mathfrak{a}$ be an ideal and M an m-system which does not meet $\mathfrak{a}$. A set $\mathfrak{q}$ of elements of R is a minimal ideal containing $\mathfrak{a}$ and having property* (A) *relative to M if and only if $C(\mathfrak{q})$ is a maximal right M-n-system which does not meet $\mathfrak{a}$.*

Proof. (i) First suppose $C(\mathfrak{q})$ is a maximal right M-n-system which does not meet $\mathfrak{a}$. By Lemma 2, $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{q}^*$ which does not meet $C(\mathfrak{q})$. Moreover, $\mathfrak{q}^*$ has property (A) relative to M and hence $C(\mathfrak{q}^*)$ is a right M-n-system which does not meet $\mathfrak{a}$. Since $\mathfrak{q}^*$ does not meet $C(\mathfrak{q})$ we have $C(\mathfrak{q}) \subseteq C(\mathfrak{q}^*)$ and hence, from the maximal property of $C(\mathfrak{q})$, it follows that $C(\mathfrak{q}) = C(\mathfrak{q}^*)$ and $\mathfrak{q} = \mathfrak{q}^*$. Thus $\mathfrak{q}$ is an ideal with property (A) relative to M. Finally $\mathfrak{q}$ is a minimal such ideal, for if $\mathfrak{q} \supset \mathfrak{q}' \supseteq \mathfrak{a}$ where $\mathfrak{q}'$ has property (A) relative to M then $C(\mathfrak{q}')$ is a right M-n-system which does not meet $\mathfrak{a}$ and properly contains $C(\mathfrak{q})$, contrary to the maximal property of $C(\mathfrak{q})$.

(ii) Conversely, suppose $\mathfrak{q}$ is a minimal ideal containing $\mathfrak{a}$ and having property (A) relative to M. Then $C(\mathfrak{q})$ is a right M-n-system which does not meet $\mathfrak{a}$, and by Lemma 1 is contained in a maximal such right M-n-system N. Hence by (i) proved above $C(N)$ is a minimal ideal containing $\mathfrak{a}$ and having property (A) relative to M and since $C(\mathfrak{q}) \subseteq N$, $\mathfrak{q} \supseteq C(N)$ and by the minimal property of $\mathfrak{q}$, $\mathfrak{q} = C(N)$ whence $C(\mathfrak{q})$ is a maximal right M-n-system which does not meet $\mathfrak{a}$. This completes the proof.

THEOREM 1. *The right upper isolated M-component $\mathfrak{u}(\mathfrak{a}, M)$ of $\mathfrak{a}$ is an ideal. Its complement in R is the uniquely determined maximal right M-n-system which does not meet $\mathfrak{a}$, and $\mathfrak{u}(\mathfrak{a}, M)$ itself is the crosscut of all ideals containing $\mathfrak{a}$ which have property* (A) *relative to M.*

Proof. Let M be an m-system which does not meet $\mathfrak{a}$ and let N be the maximal right M-n-system not meeting $\mathfrak{a}$ whose existence is assured by Lemma 1. By Lemma 3, $\mathfrak{q} = C(N)$ is a minimal ideal containing $\mathfrak{a}$ and having property (A) relative to M. Since the crosscut of any set of ideals containing $\mathfrak{a}$ and having property (A) again has property (A) it follows that there is a unique minimal such ideal which must be equal to $\mathfrak{q}$ and hence $\mathfrak{q}$ is the crosscut of all ideals containing $\mathfrak{a}$ which have property (A) relative to M. It remains to prove that $\mathfrak{q} = \mathfrak{u}(\mathfrak{a}, M)$.

First, $\mathfrak{q} \subseteq \mathfrak{u}(\mathfrak{a}, M)$. For if $x \in \mathfrak{q}$ then x does not belong to N, the maximal right M-n-system which does not meet $\mathfrak{a}$. Hence every M-n-system which contains x meets $\mathfrak{a}$ and $x \in \mathfrak{u}(\mathfrak{a}, M)$. On the other hand, $\mathfrak{u}(\mathfrak{a}, M) \subseteq \mathfrak{q}$. For if $x \in \mathfrak{u}(\mathfrak{a}, M)$ then x cannot belong to N and must belong to $\mathfrak{q}$. Hence $\mathfrak{u}(\mathfrak{a}, M) = \mathfrak{q}$ and the theorem is proved.

COROLLARY 1. *If $\mathfrak{a} \supseteq \mathfrak{b}$ and M is an m-system which does not meet $\mathfrak{a}$ then $\mathfrak{u}(\mathfrak{a}, M) \supseteq \mathfrak{u}(\mathfrak{b}, M)$.*

COROLLARY 2. *If M_1, M_2, are m-systems which do not meet $\mathfrak{a}$ and if $M_1 \supseteq M_2$ then $\mathfrak{u}(\mathfrak{a}, M_1) \supseteq \mathfrak{u}(\mathfrak{a}, M_2)$.*

Proof. Every M_1-n-system is also an M_2-n-system and hence the maximal M_1-n-system which does not meet $\mathfrak{a}$ is contained in the maximal such M_2-n-system. Taking complements,

$$\mathfrak{u}(\mathfrak{a}, M_1) \supseteq \mathfrak{u}(\mathfrak{a}, M_2).$$

If $\mathfrak{p}$ is a prime ideal which divides $\mathfrak{a}$ and if $M = C(\mathfrak{p})$, then $\mathfrak{u}(\mathfrak{a}, M)$ will also be referred to as the right upper $\mathfrak{p}$-component of $\mathfrak{a}$ and will also be denoted, when convenient, by $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$.

3. Lower isolated component ideals. In this section we shall define a right lower isolated component of an ideal $\mathfrak{a}$, and we shall investigate its relationship to the upper isolated component discussed in the previous section.

DEFINITION 3.1. *If $\mathfrak{a}$ is any ideal in R and M any m-system which does not meet $\mathfrak{a}$, the right lower isolated component of $\mathfrak{a}$ coresponding to M, or briefly the right*

lower M-component of $\mathfrak{a}$, is defined to be the set of all elements x of R such that $xRm \subseteq \mathfrak{a}$ for some element m of M.

The right lower M-component of $\mathfrak{a}$ will be denoted by $\mathfrak{l}(\mathfrak{a}, M)$. It is clear that $\mathfrak{l}(\mathfrak{a}, M)$ is an ideal, for if $x \in \mathfrak{l}(\mathfrak{a}, M)$ certainly, $-x$, and rx and xr belong to $\mathfrak{l}(\mathfrak{a}, M)$ for all r in R. Also if $x_1Rm_1 \subseteq \mathfrak{a}$ and $x_2Rm_2 \subseteq \mathfrak{a}$ where m_1, m_2 belong to M, then $m_1rm_2 \in M$ for some r in R and

$$(x_1 + x_2)Rm_1rm_2 \subseteq x_1Rm_1rm_2 + x_2Rm_2 \subseteq \mathfrak{a}.$$

Hence $x_1 + x_2 \in \mathfrak{l}(\mathfrak{a}, M)$.

THEOREM 2. *If $\mathfrak{a}$ is an ideal and M an m-system which does not meet $\mathfrak{a}$ then $\mathfrak{u}(\mathfrak{a}, M) \supseteq \mathfrak{l}(\mathfrak{a}, M) \supseteq \mathfrak{a}$.*

Proof. If $x \in \mathfrak{l}(\mathfrak{a}, M)$ then $xRm \subseteq \mathfrak{a}$ for some element m of M. Hence every right M-n-system which contains x meets $\mathfrak{a}$ and $x \in \mathfrak{u}(\mathfrak{a}, M)$. That $\mathfrak{l}(\mathfrak{a}, M) \supseteq \mathfrak{a}$ is obvious from the definition.

THEOREM 3.

(a) $\mathfrak{u}[\mathfrak{u}(\mathfrak{a}, M), M] = \mathfrak{u}(\mathfrak{a}, M)$,

(b) $\mathfrak{l}[\mathfrak{u}(\mathfrak{a}, M), M] = \mathfrak{u}(\mathfrak{a}, M)$,

(c) $\mathfrak{u}[\mathfrak{l}(\mathfrak{a}, M), M] = \mathfrak{u}(\mathfrak{a}, M)$.

Proof. (a) The complement in R of $\mathfrak{u}(\mathfrak{a}, M)$ is a right M-n-system N and hence is certainly the maximal such that does not meet $\mathfrak{u}(\mathfrak{a}, M)$. Hence by Theorem 1, $C(N) = \mathfrak{u}(\mathfrak{a}, M)$ is the right upper M-component of $\mathfrak{u}(\mathfrak{a}, M)$.

(b) The ideal $\mathfrak{l}[\mathfrak{u}(\mathfrak{a}, M), M]$ consists of all elements x of R such that $xRm \subseteq \mathfrak{u}(\mathfrak{a}, M)$ for some m in M. But since $\mathfrak{u}(\mathfrak{a}, M)$ has property (A) relative to M this implies that $x \in \mathfrak{u}(\mathfrak{a}, M)$. Hence $\mathfrak{l}[\mathfrak{u}(\mathfrak{a}, M), M] \subseteq \mathfrak{u}(\mathfrak{a}, M)$. Since, by Theorem 2, $\mathfrak{u}(\mathfrak{a}, M) \subseteq \mathfrak{l}[\mathfrak{u}(\mathfrak{a}, M), M]$, the equality follows.

(c) If $x \in \mathfrak{u}[\mathfrak{l}(\mathfrak{a}, M), M]$ then every right M-n-system N which contains x meets $\mathfrak{l}(\mathfrak{a}, M)$, that is, N contains an element n such that $nRm \subseteq \mathfrak{a}$ for some m in M. But since $n \in N$ and $m \in M$, $nrm \in N$ for some r in R. Hence N meets $\mathfrak{a}$ and $x \in \mathfrak{u}(\mathfrak{a}, M)$ and we have $\mathfrak{u}[\mathfrak{l}(\mathfrak{a}, M), M] \subseteq \mathfrak{u}(\mathfrak{a}, M)$. But since $\mathfrak{a} \subseteq \mathfrak{l}(\mathfrak{a}, M)$, by Corollary 1, Theorem 1, $\mathfrak{u}(\mathfrak{a}, M) \subseteq \mathfrak{u}[\mathfrak{l}(\mathfrak{a}, M), M]$ and the equality follows.

DEFINITION 3.2. *For all ordinal numbers $\mathfrak{a}$ we define the ideal $\mathfrak{l}^{\mathfrak{a}}(\mathfrak{a}, M)$ by induction as follows: $\mathfrak{l}^1(\mathfrak{a}, M) = \mathfrak{l}(\mathfrak{a}, M)$. If $\mathfrak{a}$ is not a limit ordinal, $\mathfrak{l}^{\mathfrak{a}}(\mathfrak{a}, M) = \mathfrak{l}[\mathfrak{l}^{\mathfrak{a}-1}(\mathfrak{a}, M), M]$, while if $\mathfrak{a}$ is a limit ordinal, $\mathfrak{l}^{\mathfrak{a}}(\mathfrak{a}, M)$ is the union of all $\mathfrak{l}^{\sigma}(\mathfrak{a}, M)$ for which $\sigma < \mathfrak{a}$.*

It is clear that $\mathfrak{l}^{\mathfrak{a}}(\mathfrak{a}, M) \supseteq \mathfrak{l}^{\sigma}(\mathfrak{a}, M)$ if $\sigma < \mathfrak{a}$.

THEOREM 4. *For all ordinal numbers $\mathfrak{a}$, $\mathfrak{u}(\mathfrak{a}, M) \supseteq \mathfrak{l}^{\mathfrak{a}}(\mathfrak{a}, M)$.*

Proof. By Theorem 2 the result is known for $\mathfrak{a} = 1$. We assume the theorem for all ordinals less than $\mathfrak{a}$ and proceed by induction.

Case 1. If $\mathfrak{a}$ is not a limit ordinal and so has an immediate predecessor $\mathfrak{a} - 1$ we have

$$\begin{aligned}
\mathfrak{l}^{\alpha}(\mathfrak{a}, M) &= \mathfrak{l}[\mathfrak{l}^{\alpha-1}(\mathfrak{a}, M), M] \\
&\subseteq \mathfrak{u}[\mathfrak{l}^{\alpha-1}(\mathfrak{a}, M), M] && \text{by Theorem 2,} \\
&\subseteq \mathfrak{u}[\mathfrak{u}(\mathfrak{a}, M), M] && \text{by Corollary 1, Theorem 1,} \\
&= \mathfrak{u}(\mathfrak{a}, M) && \text{by Theorem 3(a).}
\end{aligned}$$

Case 2. If α is a limit ordinal $\mathfrak{l}^{\alpha}(\mathfrak{a}, M)$ is the union of all $\mathfrak{l}^{\sigma}(\mathfrak{a}, M)$ for $\sigma < \alpha$. Hence if $x \in \mathfrak{l}^{\alpha}(\mathfrak{a}, M)$ then $x \in \mathfrak{l}^{\sigma}(\mathfrak{a}, M)$ for $\sigma < \alpha$ and $x \in \mathfrak{u}(\mathfrak{a}, M)$ by the induction assumption, and hence $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) \subseteq \mathfrak{u}(\mathfrak{a}, M)$.

THEOREM 5. *For any ordinal number* α, $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{l}^{\alpha+1}(\mathfrak{a}, M)$ *if and only if* $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$.

Proof. (i) If $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$ then $\mathfrak{l}^{\alpha+1}(\mathfrak{a}, M) = \mathfrak{l}[\mathfrak{u}(\mathfrak{a}, M), M] = \mathfrak{u}(\mathfrak{a}, M)$ by Theorem 3(b).

(ii) If $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{l}^{\alpha+1}(\mathfrak{a}, M)$, let x be any element of $\mathfrak{l}^{\alpha+1}(\mathfrak{a}, M)$ so that $xRm \subseteq \mathfrak{l}^{\alpha}(\mathfrak{a}, M)$ for some element m of M. But under the assumption $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{l}^{\alpha+1}(\mathfrak{a}, M)$ the condition $xRm \subseteq \mathfrak{l}^{\alpha}(\mathfrak{a}, M)$ implies $x \in \mathfrak{l}^{\alpha}(\mathfrak{a}, M)$. Hence $\mathfrak{l}^{\alpha}(\mathfrak{a}, M)$ has property (A) relative to M and since $\mathfrak{u}(\mathfrak{a}, M)$ is the minimal ideal having this property we have $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$.

COROLLARY 1. *There exists an ordinal number* α, *finite or transfinite, such that* $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$.

Since the $\mathfrak{l}^{\sigma}(\mathfrak{a}, M)$ are well ordered and the union of every subset of them is again an $\mathfrak{l}^{\sigma}(\mathfrak{a}, M)$, by Zorn's lemma they are all contained in a maximal one, $\mathfrak{l}^{\alpha}(\mathfrak{a}, M)$. Necessarily $\mathfrak{l}^{\alpha}(\mathfrak{a}, M) = \mathfrak{l}^{\alpha+1}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$ by the theorem.

COROLLARY 2. *If the ascending chain condition holds in the residue class ring* $R/\mathfrak{a}$ *then* $\mathfrak{l}^{n}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$ *for some finite* n.

COROLLARY 3. *If the ascending chain condition holds in* $R/\mathfrak{a}$ *and if* $x \in \mathfrak{u}(\mathfrak{a}, M)$ *then for every element* r *of* R *there exists an element* m_r *of* M *such that* $xrm_r \in \mathfrak{a}$. *The element* m_r *is independent of* r *if and only if* $\mathfrak{l}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$.

Proof. By Corollary 1, $\mathfrak{l}^{n}(\mathfrak{a}, M) = \mathfrak{u}(\mathfrak{a}, M)$. Hence, if $x \in \mathfrak{u}(\mathfrak{a}, M)$ there exists an element m of M such that $xRm \subseteq \mathfrak{l}^{n-1}(\mathfrak{a}, M)$. That is, for every r_1 in R there is an element $m(r_1)$ of M such that

$$xr_1mRm(r_1) \subseteq \mathfrak{l}^{n-2}(\mathfrak{a}, M).$$

Hence for every r_2 in R there is an element $m(r_2)$ such that

$$xr_1mr_2m(r_1)Rm(r_2) \subseteq \mathfrak{l}^{n-3}(\mathfrak{a}, M).$$

Carrying on in this way we find

$$xr_1mr_2m(r_1)r_3m(r_2) \ldots r_{n-1}m(r_{n-2})Rm(r_{n-1}) \subseteq \mathfrak{a}.$$

Now r_3 can be chosen so that $mr_2m(r_1) \in M$; r_4 so that $mr_3m(r_1)r_3m(r_2) \in M$ and so on. Finally, choose r_n so that $mr_2m(r_1)r_3m(r_2) \ldots (r_{n-2})r_nm(r_{n-1}) \in M$ and the result follows.

Finally, if for all x in $\mathfrak{u}(\mathfrak{a}, M)$, $xrm \in \mathfrak{a}$ where m is independent of r then $xRm \subseteq \mathfrak{a}$ and $x \in \mathfrak{l}(\mathfrak{a}, M)$ and $\mathfrak{u}(\mathfrak{a}, M) = \mathfrak{l}(\mathfrak{a}, M)$. Conversely, if $\mathfrak{u}(\mathfrak{a}, M) = \mathfrak{l}(\mathfrak{a}, M)$ then there exists an m independent of r and the proof of the corollary is complete.

4. The commutative case. We shall now investigate the relationship of $\mathfrak{l}(\mathfrak{a}, M)$ and $\mathfrak{u}(\mathfrak{a}, M)$ to the isolated component ideals defined by Krull [4, p. 16] in a commutative ring.

THEOREM 6. *If $\mathfrak{a}$ is an ideal in a commutative ring R, and M an m-system which does not meet $\mathfrak{a}$, the set $\mathfrak{a}(M)$ of all elements x of R for which $xm \in \mathfrak{a}$ for some element m of M, is an ideal.*

Proof. If $xm_1 \in \mathfrak{a}$ and $ym_2 \in \mathfrak{a}$ where m_1 and m_2 are elements of M, then if r is chosen so that $m_1rm_2 \in M$ we have

$$(x - y)m_1rm_2 = xm_1rm_2 - ym_2m_1r \in \mathfrak{a}.$$

and therefore $x - y \in \mathfrak{a}(M)$. Since obviously $cx \in \mathfrak{a}(M)$ for all c in R, $\mathfrak{a}(M)$ is an ideal.

DEFINITION 4.1. *The ideal $\mathfrak{a}(M)$ defined in Theorem 6 is called the isolated M-component of $\mathfrak{a}$.*

The isolated component ideal of Krull was defined exactly as in Definition 4.1 except that M was restricted to be a multiplicatively closed system. Since every multiplicatively closed system is an m-system [5] our definition of $\mathfrak{a}(M)$ coincides with that of Krull whenever the latter applies, that is, whenever M is multiplicatively closed. That $\mathfrak{u}(\mathfrak{a}, M)$ and $\mathfrak{l}(\mathfrak{a}, M)$ may both be considered as generalizations of $\mathfrak{a}(M)$ to the noncommutative case may now be seen from the following result.

THEOREM 7. *If $\mathfrak{a}$ is any ideal in a commutative ring R, and M is an m-system which does not meet $\mathfrak{a}$, then $\mathfrak{u}(\mathfrak{a}, M) = \mathfrak{l}(\mathfrak{a}, M) = \mathfrak{a}(M)$.*

Proof. If $x \in \mathfrak{a}(M)$ then $xm \in \mathfrak{a}$ for some element m of M. Hence, since R is commutative, $xRm \subseteq \mathfrak{a}$. Therefore $x \in \mathfrak{l}(\mathfrak{a}, M)$, and $\mathfrak{a}(M) \subseteq \mathfrak{l}(\mathfrak{a}, M)$.

Now if $x \in \mathfrak{u}(\mathfrak{a}, M)$, every M-n-system which contains x meets $\mathfrak{a}$. But the set of elements $N = \{x, M, xm\}$ containing x, M, and all elements xm where $m \in M$, is an M-n-system containing x. Hence N meets $\mathfrak{a}$ and since M does not meet $\mathfrak{a}$ it follows that $xm \in \mathfrak{a}$ for some element m of M. Therefore $x \in \mathfrak{a}(M)$ and we have now $\mathfrak{u}(\mathfrak{a}, M) \subseteq \mathfrak{a}(M) \subseteq \mathfrak{l}(\mathfrak{a}, M)$. But by Theorem 2, $\mathfrak{l}(\mathfrak{a}, M) \subseteq \mathfrak{u}(\mathfrak{a}, M)$ and the theorem follows.

5. Chain conditions. For most of what follows it will be necessary to assume that the ring R satisfies the ascending chain condition for two sided ideals. Before imposing this restriction, however, we shall develop some consequences of the following weak form of the descending chain condition.

CONDITION A. *For every ideal* $\mathfrak{a}$ *which is not prime, the ring* $R/\mathfrak{a}$ *satisfies the descending chain condition for two sided ideals.*

THEOREM 8. *If* $\mathfrak{s}$ *is a minimal proper divisor of* $\mathfrak{a}$ *then* $\mathfrak{s}^{-1}\mathfrak{a}$ *is a prime divisor of* $\mathfrak{a}$ *and is not right prime to* $\mathfrak{a}$.

Proof. If $\mathfrak{s}^{-1}\mathfrak{a} = R$, it is prime, and since $\mathfrak{s}R(\mathfrak{s}^{-1}\mathfrak{a}) \subseteq \mathfrak{a}$ and $\mathfrak{s}$ is a proper divisor of $\mathfrak{a}$ it follows that $\mathfrak{s}^{-1}\mathfrak{a}$ is nrp to $\mathfrak{a}$. ("nrp" means "not right prime.")

If $\mathfrak{s}^{-1}\mathfrak{a} \neq R$, suppose $xRy \subseteq \mathfrak{s}^{-1}\mathfrak{a}$ where x is not in $\mathfrak{s}^{-1}\mathfrak{a}$. Then for every element s of $\mathfrak{s}$, $sRxRy \subseteq \mathfrak{a}$, but for some element s' of $\mathfrak{s}$, $s'Rx$ not $\subseteq \mathfrak{a}$. Choose r in R so that $s'rx$ is not in $\mathfrak{a}$ and form the ideal $(s'rx, \mathfrak{a})$ which properly contains $\mathfrak{a}$ but is contained in $\mathfrak{s}$. From the minimal property of $\mathfrak{s}$ we have therefore $\mathfrak{s} = (s'rx, \mathfrak{a})$ and every element s of $\mathfrak{s}$ has the form

$$s = a + is'rx + r_1s'rx + s'rxr_2 + \sum_{i,j} r_is'rxr_j,$$

where $a \in \mathfrak{a}$, i is an integer and r_1, r_2, r_i, r_j are elements of R. Since $s'RxRy \subseteq \mathfrak{a}$ it is clear from the form of the above expression for s that $sRy \subseteq \mathfrak{a}$ and hence $y \in \mathfrak{s}^{-1}\mathfrak{a}$. Thus if x is not in $\mathfrak{s}^{-1}\mathfrak{a}$ and $xRy \subseteq \mathfrak{s}^{-1}\mathfrak{a}$ then $y \in \mathfrak{s}^{-1}\mathfrak{a}$ and hence $\mathfrak{s}^{-1}\mathfrak{a}$ is prime. Since $\mathfrak{s}$ contains an element s not in $\mathfrak{a}$ and since $sR(\mathfrak{s}^{-1}\mathfrak{a}) \subseteq \mathfrak{a}$ it is clear that $\mathfrak{s}^{-1}\mathfrak{a}$ is nrp to $\mathfrak{a}$.

COROLLARY. *If condition* A *holds in* R *then every ideal* $\mathfrak{a} \neq R$ *has a minimal prime divisor which is not right prime to* $\mathfrak{a}$.

For condition A ensures the existence of a minimal ideal containing $\mathfrak{a}$ and hence a prime $\mathfrak{p}$ which is nrp to $\mathfrak{a}$. This prime must contain a minimal prime divisor of $\mathfrak{a}$ which will also be nrp to $\mathfrak{a}$.

THEOREM 9. *If the ascending chain condition holds for two sided ideals in* R *then every ideal* $\mathfrak{c}$ *in* R *has at most a finite number of minimal prime divisors* [2].

Proof. If $\mathfrak{c}$ is a prime ideal the theorem is obvious. If $\mathfrak{c}$ is not prime there exist elements a_1, and b_1 of R which do not belong to $\mathfrak{c}$ such that $a_1Rb_1 \subseteq \mathfrak{c}$. Hence if $\mathfrak{c}$ is contained in an infinite number of minimal primes $\mathfrak{p}_i$ either a_1 or b_1 must belong to an infinite number of these. Suppose it is a_1 and let $\mathfrak{a}_1 = (a_1, \mathfrak{c})$. Then $\mathfrak{a}_1$ is a proper divisor of $\mathfrak{c}$, $\mathfrak{p}_i \supseteq \mathfrak{a}_1$ for an infinite number of primes $\mathfrak{p}_i$, and each of these $\mathfrak{p}_i$ is a minimal prime divisor of $\mathfrak{a}_1$. Hence $\mathfrak{a}_1$ cannot be prime. Therefore if $\mathfrak{c}$ has an infinite number of minimal prime divisors it has a proper divisor with the same property and continuation of this argument leads to a contradiction of the ascending chain condition in R.

THEOREM 10. *If the ascending chain condition holds for two sided ideals in* R *and* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ *are the minimal prime divisors of an ideal* $\mathfrak{c}$ *then*

$$\mathfrak{p}_{i_1}R\mathfrak{p}_{i_2}R \ldots R\mathfrak{p}_{i_m} \subseteq \mathfrak{c}$$

where $i_1, i_2, \ldots, i_m$ *is some finite permutation of the integers* $1, 2, \ldots, n$ *with repetitions allowed.*

Proof. The theorem is trivially true if $\mathfrak{c}$ is prime. If $\mathfrak{c}$ is not prime, there exist elements a and b not in $\mathfrak{c}$ such that $aRb \subseteq \mathfrak{c} \subset \mathfrak{p}_i$ $(i = 1, 2, \ldots, n)$. Hence for each i either $a \in \mathfrak{p}_i$ or $b \in \mathfrak{p}_i$. Form the ideals $\mathfrak{a}_1 = (a, \mathfrak{c})$ and $\mathfrak{b}_1 = (b, \mathfrak{c})$ both of which are proper divisors of $\mathfrak{c}$. Let $\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_r$ be the minimal prime divisors of $\mathfrak{a}_1$ and $\mathfrak{p}''_1, \mathfrak{p}''_2, \ldots, \mathfrak{p}''_r$ be those of $\mathfrak{b}_1$. Now suppose that both $\mathfrak{a}_1$ and $\mathfrak{b}_1$ have the property that we wish to prove of $\mathfrak{c}$, so that $\mathfrak{p}'_{i_1} R \mathfrak{p}'_{i_2} R \ldots R\mathfrak{p}'_{i_q} \subseteq \mathfrak{a}_1$ and $\mathfrak{p}''_{k_1} R \mathfrak{p}''_{k_2} R \ldots R\mathfrak{p}''_{k_t} \subseteq \mathfrak{b}_1$ and hence, since $a, Rb_1 \subseteq \mathfrak{c}$,

$$\mathfrak{p}'_{i_1} R \mathfrak{p}'_{i_2} R \ldots R\mathfrak{p}'_{i_q} R \mathfrak{p}''_{k_1} R \ldots R\mathfrak{p}''_{k_t} \subseteq \mathfrak{c}.$$

Now each $\mathfrak{p}'_i$ and $\mathfrak{p}''_k$, being a prime divisor of $\mathfrak{c}$, contains a minimal prime of $\mathfrak{c}$, and hence $\mathfrak{p}_{i_1} R \mathfrak{p}_{i_2} R \ldots R\mathfrak{p}_{i_m} \subseteq \mathfrak{c}$ where $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}$ are minimal primes of $\mathfrak{c}$. Hence if the theorem is false for $\mathfrak{c}$ it is false for a proper divisor of $\mathfrak{c}$, and a continuation of this argument leads to a contradiction of the ascending chain condition in R.

COROLLARY. *If the ascending chain condition holds for two sided ideals in R then every ideal $\mathfrak{a} \neq R$ has a minimal prime divisor which is not right prime to $\mathfrak{a}$.*

Proof. If $\mathfrak{a}$ is prime but $\neq R$ then $\mathfrak{a}$ itself is the required minimal prime. If $\mathfrak{a}$ is not prime, by Theorem 10 we have

$$\mathfrak{p}_1 R \mathfrak{p}_2 R \ldots R\mathfrak{p}_s \subseteq \mathfrak{a} \tag{1}$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ are (not necessarily distinct) minimal primes of $\mathfrak{a}$ and $s > 1$. Hence there exists a shortest product of the form (1) which belongs to $\mathfrak{a}$; that is, there exists an $s > 1$ such that (1) holds but

$$\mathfrak{p}_1 R \mathfrak{p}_2 R \ldots R\mathfrak{p}_{s-1} \text{ not} \subseteq \mathfrak{a}.$$

It follows that $\mathfrak{p}_s$ is nrp to $\mathfrak{a}$.

6. Primary ideals. In this section we shall require the results of [5] concerning the radical of an ideal. The radical $\mathfrak{r}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is defined as the set of all elements x of R such that every m-system containing x meets $\mathfrak{a}$. McCoy has shown that $\mathfrak{r}(\mathfrak{a})$ is an ideal and is equal to the intersection of all minimal prime divisors of $\mathfrak{a}$.

DEFINITION 6.1. *An ideal $\mathfrak{q}$ is said to be right primary if all elements not in $\mathfrak{r}(\mathfrak{q})$ are right prime to $\mathfrak{q}$.*

Thus $\mathfrak{q}$ is right primary if the conditions $aRb \subseteq \mathfrak{q}$ and $b \notin \mathfrak{r}(\mathfrak{q})$ together imply $a \in \mathfrak{q}$.

THEOREM 11. *If either Condition* A *or the ascending chain condition holds in R then the radical of a right primary ideal is prime.*

Proof. Suppose $\mathfrak{q}$ is right primary. By the corollaries to Theorems 8 and 10, if $\mathfrak{q} \neq R$ it has a minimal prime divisor $\mathfrak{p}$ which is nrp to $\mathfrak{q}$. Hence for every element p of $\mathfrak{p}$ we have $xRp \subseteq \mathfrak{q}$ for some x not in $\mathfrak{q}$. Since $\mathfrak{q}$ is right primary

this implies that $p \in \mathfrak{r}(\mathfrak{q})$ and hence $\mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{q})$. But since $\mathfrak{r}(\mathfrak{q})$ is the intersection of the minimal primes of $\mathfrak{q}$ we have $\mathfrak{r}(\mathfrak{q}) \subseteq \mathfrak{p}$ and the theorem follows. If $\mathfrak{q} = R$ then $\mathfrak{r}(\mathfrak{q}) = R$ and the theorem holds in this case too.

In rings which satisfy no finite chain conditions it seems possible that right primary ideals may exist whose radical is not prime. Such an ideal $\mathfrak{q}$, if it exists, must be such that all its minimal prime divisors are right prime to $\mathfrak{q}$ and no product of the form $\mathfrak{p}_1 R\mathfrak{p}_2 R \ldots R\mathfrak{p}_n$, where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ are (not necessarily distinct) minimal prime divisors of $\mathfrak{q}$, can belong to $\mathfrak{q}$. Since, in a commutative ring, every minimal prime divisor of $\mathfrak{q}$ is nrp to $\mathfrak{q}$ [6, p. 112] our definition of a (right) primary ideal implies a prime radical in the commutative case even without chain conditions. In fact, in a commutative ring it reduces to the usual definition of a primary ideal by virtue of [6, p. 182, Theorem 59].

7. Ideals expressible as the intersection of right primary ideals. In this section we shall consider ideals which can be represented as the intersection of a finite number of right primary ideals and shall find what characteristics of such a representation are uniquely determined by the ideal in question. It will be assumed throughout the remainder of the paper that the ascending chain condition holds for the two sided ideals of R. A representation

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r \tag{2}$$

of an ideal $\mathfrak{a}$ as the intersection of right primary ideals, $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ will be called an irredundant representation if no one of the ideals $\mathfrak{q}_i$ contains the intersection of the remaining ones.

THEOREM 12. *If* (2) *is an irredundant representation of an ideal* $\mathfrak{a}$ *as the intersection of right primary ideals* $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, *then an element* x *is right prime to* $\mathfrak{a}$ *if and only if* $x \in C(\mathfrak{p}_i)$ *for* $i = 1, 2, \ldots, r$, *where* $\mathfrak{p}_i$ *is the radical of* $\mathfrak{q}_i$.

Proof. (i) If a is nrp to $\mathfrak{a}$ then for some element x which is not in $\mathfrak{a}$, $xRa \subseteq \mathfrak{a}$. But this implies $xRa \subseteq \mathfrak{q}_i$ for $i = 1, 2, \ldots, r$ while $x \notin \mathfrak{q}_j$ for at least one value of j. Hence, since $\mathfrak{q}_j$ is right primary, $a \in \mathfrak{p}_j$. It follows that if $a \in C(\mathfrak{p}_i)$ for all i then a is right prime to $\mathfrak{a}$.

(ii) Conversely, suppose that a is an element of at least one of the primes $\mathfrak{p}_i$ and let it be $\mathfrak{p}_1$. By Theorem 10 some product of the form

$$aRaR \ldots aRa$$

is contained in $\mathfrak{q}_1$. Since the representation $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ is irredundant we can choose an element b which is contained in $\mathfrak{q}_2 \cap \mathfrak{q}_3 \cap \ldots \cap \mathfrak{q}_r$ but not in $\mathfrak{q}_1$. Then

$$bRaR \ldots aRa \subseteq \mathfrak{a}.$$

Suppose the shortest such product which is contained in $\mathfrak{a}$ has s factors a. Then $s \geqslant 1$ since $b \notin \mathfrak{a}$. If $s = 1$ then $bRa \subseteq \mathfrak{a}$ and therefore a is nrp to $\mathfrak{a}$. If $s > 1$ then the product $bRaR \ldots aRa$, with $s - 1$ factors a, contains an element b'

which does not belong to $\mathfrak{a}$, while $b'Ra \subseteq \mathfrak{a}$, and again, a is nrp to $\mathfrak{a}$. This completes the proof.

THEOREM 13. *The intersection of any finite number of right primary ideals all of which have the same radical $\mathfrak{p}$ is a right primary ideal with radical $\mathfrak{p}$.*

Proof. Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ be right primary ideals all having radical $\mathfrak{p}$ and let $\mathfrak{q}$ be their intersection. Since $\mathfrak{p}$ is the only nimimal prime divisor of $\mathfrak{q}_i$ we have by Theorem 10 that $\mathfrak{p}R\mathfrak{p}R \ldots \mathfrak{p}R\mathfrak{p}$ is contained in each $\mathfrak{q}_i$ and hence $\mathfrak{p}R\mathfrak{p}R \ldots \mathfrak{p}R\mathfrak{p} \subseteq \mathfrak{q}$. Therefore, if $\mathfrak{p}_1$ is any prime divisor of $\mathfrak{q}$ we have $\mathfrak{p}_1 \supseteq \mathfrak{p}R\mathfrak{p}R \ldots \mathfrak{p}R\mathfrak{p}$ and hence $\mathfrak{p}_1 \supseteq \mathfrak{p}$ by the definition of a prime ideal. It follows that $\mathfrak{p}$ is a unique minimal prime divisor of $\mathfrak{q}$ and therefore $\mathfrak{p} = \mathfrak{r}(\mathfrak{q})$. Moreover, if $aRb \subseteq \mathfrak{q}$ and $a \notin \mathfrak{q}$ then $aRb \subseteq \mathfrak{q}_i$ for each i while $a \notin \mathfrak{q}_j$ for at least one j. Since $\mathfrak{q}_i$ is right primary with radical $\mathfrak{p}$ this implies that $b \in \mathfrak{p} = \mathfrak{r}(\mathfrak{q})$ whence $\mathfrak{q}$ is right primary with radical $\mathfrak{p}$.

THEOREM 14. *An irredundant intersection of a finite number of right primary ideals not all of which have the same radical is not a right primary ideal.*

Proof. Let $\mathfrak{q}$ be an irredundant intersection of right primary ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ whose radicals are $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. If $\mathfrak{q}$ is right primary it has a unique minimal prime divisor $\mathfrak{p}$ and all elements not in $\mathfrak{p}$ are right prime to $\mathfrak{q}$. But by Theorem 12, if x is right prime to $\mathfrak{q}$, x is not contained in any of the primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Hence $C(\mathfrak{p}) \subseteq C(\mathfrak{p}_i)$ and $\mathfrak{p} \supseteq \mathfrak{p}_i$ for $i = 1, 2, \ldots, r$. Since $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{q}$ it follows that each $\mathfrak{p}_i$ is equal to $\mathfrak{p}$. Hence if $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are not all equal $\mathfrak{q}$ is not right primary.

DEFINITION 7.1. *An irredundant representation* (2) *of $\mathfrak{a}$ will be called a short representation if none of the ideals obtained by taking the intersection of two or more of the ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ are right primary.*

In view of Theorems 13 and 14 the irredundant representation (2) is a short representation of $\mathfrak{a}$ if and only if no two of the radicals of $\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_r$ are equal.

THEOREM 15. *Let $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_n$ be an irredundant representation of $\mathfrak{a}$ as the intersection of right primary ideals, and let $\mathfrak{p}_i$ be the radical of $\mathfrak{q}_i$. If $\mathfrak{p}$ is a prime ideal not equal to R which contains $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ but does not contain $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_n$, then $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$.*

Proof. If $\mathfrak{p} \supseteq \mathfrak{p}_i$ then by Theorem 1, Corollary 2,

$$\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) \subseteq \mathfrak{u}(\mathfrak{a}, \mathfrak{p}_i).$$

But since $\mathfrak{q}_i$ has property (A) relative to the m-system $C(\mathfrak{p}_i)$, Theorem 1 shows that $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}_i) \subseteq \mathfrak{q}_i$. Hence

$$\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r. \tag{3}$$

Now if $r = n$, (3) gives $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) \subseteq \mathfrak{a}$ and since $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) \supseteq \mathfrak{a}$ we have $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = \mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_n$ and the result is proved in this case. If $r < n$, since $\mathfrak{p}$

does not contain $\mathfrak{p}_i$ for $j > r$, it follows that $\mathfrak{p}$ does not contain $\mathfrak{q}_i$ either; for since $\mathfrak{p}_i$ is the only minimal prime of $\mathfrak{q}_i$ it is contained in every prime which contains $\mathfrak{q}_i$. Hence there exist elements $m_1, m_2, \ldots m_{n-r}$ such that $m_i \in \mathfrak{q}_{r+i}$ but $m_i \notin \mathfrak{p}$ $(i = 1, 2, \ldots, n - r)$. Now since $m_1, m_2, \ldots, m_{n-r}$ all belong to the m-system $M = C(\mathfrak{p})$, there exist elements $x_1, x_2, \ldots, x_{n-r-1}$ such that the element $m = m_1 x_1 m_2 x_2 m_3 \ldots x_{n-r-1} m_{n-r}$ is contained in M. Also it is clear that $m \in \mathfrak{q}_{r+1} \cap \mathfrak{q}_{r+2} \cap \ldots \cap \mathfrak{q}_n$. Hence if $q \in \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ we have $qRm \subseteq \mathfrak{a}$ where $m \in M$ and therefore every right M-n-system which contains q meets $\mathfrak{a}$. Hence $q \in \mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ and

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r \subseteq \mathfrak{u}(\mathfrak{a}, \mathfrak{p}),$$

which with (3) gives the result stated in the theorem.

THEOREM 16. *If* (2) *is an irredundant representation of* $\mathfrak{a}$ *as the intersection of right primary ideals* $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ *with radicals* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$, *then the minimal prime divisors of* $\mathfrak{a}$ *are exactly those primes which are minimal in the set* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$.

Proof. For each i some product $\mathfrak{p}_i R \mathfrak{p}_i \ldots R \mathfrak{p}_i$ is contained in $\mathfrak{q}_i$. Taking products over $i = 1, 2, \ldots, r$,

$$\mathfrak{p}_{i_1} R \mathfrak{p}_{i_2} \ldots R \mathfrak{p}_{i_m} \subseteq \mathfrak{a}$$

where each $\mathfrak{p}_{i_j}$ is one of the primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Hence every prime which contains $\mathfrak{a}$ contains the above product and therefore must contain one of the primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Hence every minimal prime containing $\mathfrak{a}$ is a minimal prime of this set and conversely.

THEOREM 17. *If* (2) *is a short representation of* $\mathfrak{a}$ *as the intersection of right primary ideals* $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$, *and if*[1] $\mathfrak{p} \neq R$ *is any minimal prime divisor of* $\mathfrak{a}$, *then* $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ *is right primary and equal to one of the* $\mathfrak{q}_i$.

Proof. Since $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$, by Theorem 16 it is the radical of one of the ideals $\mathfrak{q}_i$, say $\mathfrak{q}_i$. Since $\mathfrak{p}$ is minimal it cannot contain the radical of any ideal $\mathfrak{q}_i$ for $i \neq j$. Hence Theorem 15 gives $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = \mathfrak{q}_i$.

COROLLARY 1. *If* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ *(all different from* R*) are the minimal prime divisors of* $\mathfrak{a}$ *then in any short representation of* $\mathfrak{a}$ *as the intersection of a finite number of right primary ideals,* $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}_1), \ldots, \mathfrak{u}(\mathfrak{a}, \mathfrak{p}_m)$ *must occur among the right primary components.*

COROLLARY 2. *A necessary condition that an ideal* $\mathfrak{a}$ *be representable as the intersection of a finite number of right primary ideals is that* $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}_i)$ *be right primary for all minimal prime divisors* $\mathfrak{p}_i$ *of* $\mathfrak{a}$.

DEFINITION 7.2. *If* $\mathfrak{a}$ *is representable as the intersection of right primary ideals then the upper component ideals* $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ *corresponding to the minimal prime divisors of* $\mathfrak{a}$ *are called the isolated right primary components of* $\mathfrak{a}$.

[1] The restriction $\mathfrak{p} \neq R$ excludes only the case in which $\mathfrak{a}$ is itself primary with radical R.

Thus the isolated right primary components of $\mathfrak{a}$ are right primary ideals which occur as components in every short representation of $\mathfrak{a}$ as the intersection of right primary ideals.

It is now easy to give examples of rings satisfying the ascending chain condition in which not all ideals are expressible as the intersection of a finite number of right primary ideals. Let R be the ring of all polynomials in two noncommutative indeterminates x and y with coefficients in a field K. Let $\mathfrak{a}$ be the ideal (xy) which has two minimal prime divisors $\mathfrak{p}_1 = (x)$ and $\mathfrak{p}_2 = (y)$, and is clearly not right primary. The radical of $\mathfrak{a}$ is $\mathfrak{p}_1 \cap \mathfrak{p}_2$ or (xy, yx). Now if $aRb \subseteq (xy)$ $b \notin (y)$ then $a \in (xy)$. Hence (xy) has property (A) relative to the m-system $C(\mathfrak{p}_2)$ and therefore $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}_2) = \mathfrak{a}$. Since $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}_2)$ is not right primary Theorem 17, Corollary 2, shows that $\mathfrak{a}$ is not the intersection of a finite number of right primary ideals.

Fitting's decomposition theorem [1] represents $\mathfrak{a}$ as the intersection of two "primary left ideals", namely,

$$(xy) = (x) \cap (y)_l$$

where (x) is the two sided ideal generated by x and $(y)_l$ is the left ideal generated by y. In the present paper, however, we consider only representations as intersections of two sided right primary ideals.

It can also be shown by examples that the necessary condition given in Theorem 17, Corollary 2, is not sufficient. Let R be the same ring as above and let $\mathfrak{a} = (x^2, xy)$. Then $\mathfrak{a}$ has a unique minimal prime divisor $\mathfrak{p} = (x)$ and $\mathfrak{r}(\mathfrak{a}) = (x)$. But $\mathfrak{a}$ is not right primary since $xRy \subseteq \mathfrak{a}$ while $x \notin \mathfrak{a}$ and $y \notin \mathfrak{r}(\mathfrak{a})$. Now $\mathfrak{l}(\mathfrak{a}, \mathfrak{p})$, the set of all elements r such that $rRm \subseteq \mathfrak{a}$ for some m in $C(\mathfrak{p})$, is easily seen to be equal to (x) and therefore $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) \supseteq (x)$. But (x) has property (A) relative to $C(\mathfrak{p})$ and therefore $\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = (x)$. Since $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ is right primary the necessary condition of Corollary 2 is satisfied. By Theorem 17, in any short representation of $\mathfrak{a}$ as the intersection of a finite number of right primary ideals, (x) must occur as one component. The other components must be sought among the other right primary divisors of $\mathfrak{a}$, namely, (x,y) (x^2,y), (x,y^n), (x^2,xy,y^n) and (x^2,xy,yx,y^n), $n \geqslant 2$. It is easy to verify that none of the possible finite intersections is equal to $\mathfrak{a}$.

We may note also that although $\mathfrak{a}$ is not right primary it is left primary since $aRb \subseteq (x^2,xy)$ and $a \notin (x)$ together imply $b \in (x^2,xy)$.

THEOREM 18. *If $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ is a short representation of $\mathfrak{a}$ as the intersection of right primary ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ then a prime ideal $\mathfrak{p} \neq R$ which divides $\mathfrak{a}$ is the radical of one of the ideals $\mathfrak{q}_i$ if and only if $\mathfrak{p}$ is* nrp *to $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$. The ring R is the radical of one of the $\mathfrak{q}_i$ if and only if R is* nrp *to $\mathfrak{a}$.*

Proof. (i) Let the radicals of $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ be $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. If $\mathfrak{p} = \mathfrak{p}_i$ but $\mathfrak{p} \neq R$, then by Theorem 15,

$$\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_k \tag{4}$$

where $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_k}$ are those primes among the $\mathfrak{p}_i$ which are contained in $\mathfrak{p}$. Now (4) is a short representation of $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ and $\mathfrak{p}$ is the radical of one of the ideals $\mathfrak{q}_{i_1}, \mathfrak{q}_{i_2}, \ldots, \mathfrak{q}_{i_k}$ and contains the radicals of the rest of these. Hence by Theorem 12, an element x is nrp to $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ if and only if $x \in \mathfrak{p}$. Hence if $\mathfrak{p} = \mathfrak{p}_i$ then $\mathfrak{p}$ is nrp to $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$.

(ii) Now suppose $\mathfrak{p} \supseteq \mathfrak{a}$, $\mathfrak{p} \neq R$, and $\mathfrak{p}$ is nrp to $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$. Since, by Theorem 16, all minimal prime divisors of $\mathfrak{a}$ are among the primes $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_r}$, $\mathfrak{p}$ must contain at least one of these. Suppose $\mathfrak{p}$ contains $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_k}$ but not $\mathfrak{p}_{i_{k+1}}, \ldots, \mathfrak{p}_{i_r}$. By Theorem 15,

$$\mathfrak{u}(\mathfrak{a}, \mathfrak{p}) = \mathfrak{q}_{i_1} \cap \mathfrak{q}_{i_2} \cap \ldots \cap \mathfrak{q}_{i_k}$$

is a short representation of $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$, and since $\mathfrak{p}$ is nrp to $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$ Theorem 12 gives

$$\mathfrak{p} \subseteq \mathfrak{p}_{i_1} \oplus \mathfrak{p}_{i_2} \oplus \ldots \oplus \mathfrak{p}_{i_k},$$

where $\oplus$ denotes a set-theoretic sum. But since $\mathfrak{p} \supseteq \mathfrak{p}_i$ $(i = 1, 2, \ldots, k)$ it follows that

$$\mathfrak{p} = \mathfrak{p}_{i_1} \oplus \mathfrak{p}_{i_2} \oplus \ldots \oplus \mathfrak{p}_{i_k}. \tag{5}$$

In the sum (5) any prime $\mathfrak{p}_i$ which is contained in the sum of the remaining primes may be omitted. We may assume therefore that

$$\mathfrak{p} = \mathfrak{p}_{i_1} \oplus \mathfrak{p}_{i_2} \oplus \ldots \oplus \mathfrak{p}_{i_l}, \tag{6}$$

where $l \leqslant k$ and no one of $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_l}$ is contained in the set-theoretic sum of the remaining ones.

Now if $l > 1$ the product $\mathfrak{p}_{i_1}\mathfrak{p}_{i_2} \ldots \mathfrak{p}_{i_{l-1}}$ cannot be contained in $\mathfrak{p}_{i_l}$, for if it were, since $\mathfrak{p}_{i_l}$ is prime, $\mathfrak{p}_{i_l}$ would contain one of the primes $\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \ldots, \mathfrak{p}_{i_{l-1}}$, contrary to the assumption of the minimal length of the sum (6). Hence we can choose elements p_i from $\mathfrak{p}_i$ $(i = 1, 2, \ldots, l-1)$ such that $p_{i_1}p_{i_2} \ldots p_{i_{l-1}}$ does not belong to $\mathfrak{p}_{i_l}$. Moreover, we can choose an element p_{i_l} of $\mathfrak{p}_{i_l}$ which does not belong to $\mathfrak{p}_i$ for $i < l$. Form the element $x = p_{i_1}p_{i_2} \ldots p_{i_{l-1}} + p_{i_l}$. Being the sum of two elements of $\mathfrak{p}$, $x \in \mathfrak{p}$ and therefore $x \in \mathfrak{p}_j$ for some value of j such that $1 \leqslant j \leqslant l$. But this is impossible, for if $j < l$ then $p_{i_1}p_{i_2} \ldots p_{i_{l-1}} \in \mathfrak{p}_j$ but $p_{i_l} \notin \mathfrak{p}_j$, while if $j = l$, $p_{i_l} \in \mathfrak{p}_{i_l}$ but $p_{i_1}p_{i_2} \ldots p_{i_{l-1}} \notin \mathfrak{p}_{i_l}$. This contradiction leads to the conclusion that $l = 1$ and hence $\mathfrak{p} = \mathfrak{p}_i$ for some value of i.

(iii) Suppose R is the radical of one of the $\mathfrak{q}_{i_j}$, and let it be $\mathfrak{q}_{i_1}$. Since R is therefore the only minimal prime divisor of $\mathfrak{q}_{i_1}$, Theorem 10 gives $R^s \subseteq \mathfrak{q}_{i_1}$. Choose an element q which is contained in $\mathfrak{q}_{i_2} \cap \mathfrak{q}_{i_3} \cap \ldots \cap \mathfrak{q}_{i_r}$ but not in $\mathfrak{q}_{i_1}$ so that $q \notin \mathfrak{a}$. Then $qR^s \subseteq \mathfrak{a}$. Assume s is the least exponent for which this holds, so that $s \geqslant 1$, and choose an element q' in qR^{s-1} such that q' is not contained in $\mathfrak{a}$. Then $q'Rr \subseteq \mathfrak{a}$ for all elements r of R and therefore R is nrp to $\mathfrak{a}$.

(iv) Conversely, suppose R is nrp to $\mathfrak{a}$ so that for every element r of R there is an element a_r not in $\mathfrak{a}$ such that $a_rRr \subseteq \mathfrak{a}$. Hence for each i, $a_rRr \subseteq \mathfrak{q}_i$ while for at least one j, $a_r \notin \mathfrak{q}_j$. Thus, since $\mathfrak{q}_j$ is right primary, $r \in \mathfrak{p}_j$ and

$$R = \mathfrak{p}_{i_1} \oplus \mathfrak{p}_{i_2} \oplus \ldots \oplus \mathfrak{p}_{i_r}.$$

Now let

$$R = \mathfrak{p}_1 \oplus \mathfrak{p}_2 \oplus \ldots \oplus \mathfrak{p}_l \tag{7}$$

be the sum of minimal length which is equal to R. If $l > 1$ choose $p_1, p_2, \ldots, p_l$ as above and we find the element $p_1 p_2 \ldots p_{l-1} + p_l$ belongs to none of the primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_l$, in contradiction to (7). Hence $l = 1$ and $p_i = R$ for one value of i. This completes the proof of Theorem 18.

If an ideal $\mathfrak{a}$ can be represented as the intersection of right primary ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$, Theorem 18 shows that the radicals of these right primary components are uniquely determined since the criterion given to determine whether $\mathfrak{p}$ is one of these radicals or not depends only on $\mathfrak{p}$ and $\mathfrak{a}$. Similarly the number of right primary components in a short representation is also uniquely determined as the number of distinct primes among the radicals of $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$. We may therefore summarize the results of this section as follows:

THEOREM 19. *Let R be a noncommutative ring in which the ascending chain condition holds for two sided ideals. If an ideal $\mathfrak{a}$ in R can be represented as the intersection of a finite number of right primary ideals then $\mathfrak{a}$ has a short representation as such. In any two short representations of $\mathfrak{a}$ the number of right primary components is the same and the radicals of the two sets of primary components coincide in some order. Moreover, the isolated primary components are the same for all short representations.*

Although Theorem 19 shows that the well-known results of E. Noether carry over to the noncommutative case for those ideals which can be represented as the intersection of a finite number of right primary ideals, a necessary and sufficient condition that such a representation exist is still unknown. The ascending chain condition is not sufficient to ensure this for all ideals as it is in a commutative ring. The necessary condition given by Theorem 17, Corollary 2, is not only not sufficient but is difficult to apply in a particular case owing to the difficulty of finding the ideals $\mathfrak{u}(\mathfrak{a}, \mathfrak{p})$. It is hoped to return to this problem in a later paper.

REFERENCES

1. H. Fitting, *Primarkomponentenzerlegung in nichtkommutativen Ringen*, Math. Ann., vol. 3 (1935), 19-41.
2. W. Krull, *Zur Theorie der zweiseitigen Ideale in Nichtkommutativen Bereichen*, Math. Zeit., vol. 29 (1938), 42-54.
3. ———, *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann., vol. 101 (1929), 729-744.
4. ———, *Idealtheorie*, Ergebnisse der Mathematik, vol. 4 (Berlin, 1935).
5. N. H. McCoy, *Prime ideals in general rings*, Amer. J. Math., vol. 71 (1949), 823-833.
6. ———, *Rings and ideals*, Carus Mathematical Monographs, No. 8 (Baltimore, 1948).

The University of British Columbia

NOTE ON NORMAL DECIMALS

H. DAVENPORT AND P. ERDÖS

1. Introduction. A real number, expressed as a decimal, is said to be *normal* (in the scale of 10) if every combination of digits occurs in the decimal with the proper frequency. If $a_1a_2 \dots a_k$ is any combination of k digits, and $N(t)$ is the number of times this combination occurs among the first t digits, the condition is that

$$\lim_{t\to\infty} \frac{N(t)}{t} = \frac{1}{10^k}. \tag{1}$$

It was proved by Champernowne [2] that the decimal $\cdot 1234567891011\dots$ is normal, and by Besicovitch [1] that the same holds for the decimal $\cdot 1491625\dots$. Copeland and Erdös [3] have proved that if $p_1, p_2, \dots$ is any sequence of positive integers such that, for every $\theta < 1$, the number of p's up to n exceeds n^θ if n is sufficiently large, then the infinite decimal $\cdot p_1p_2p_3\dots$ is normal. This includes the result that the decimal formed from the sequence of primes is normal.

In this note, we prove the following result conjectured by Copeland and Erdös:

THEOREM 1. *Let $f(x)$ be any polynomial in x, all of whose values, for $x = 1, 2, \dots$, are positive integers. Then the decimal $\cdot f(1)f(2)f(3)\dots$ is normal.*

It is to be understood, of course, that each $f(n)$ is written in the scale of 10, and that the digits of $f(1)$ are succeeded by those of $f(2)$, and so on. The proof is based on an interpretation of the condition (1) in terms of the equal distribution of a sequence to the modulus 1, and the application of the method of Weyl's famous memoir [6].

Besicovitch [1] introduced the concept of the (ϵ, k) normality of an individual positive integer q, where ϵ is a positive number and k is a positive integer. The condition for this is that if $a_1a_2 \dots a_l$ is any sequence of l digits, where $l \leqq k$, then the number of times this sequence occurs in q lies between

$$(1-\epsilon)10^{-l}q' \quad \text{and} \quad (1+\epsilon)10^{-l}q'$$

where q' is the number of digits in q. Naturally, the definition is only significant when q is large compared with 10^k. We prove:

THEOREM 2. *For any ϵ and k, almost all the numbers $f(1), f(2), \dots$ are (ϵ, k) normal; that is, the number of numbers $n \leqq x$ for which $f(n)$ is not (ϵ, k) normal is $o(x)$ as $x \to \infty$ for fixed ϵ and k.*

Received February 9, 1951.

This is a stronger result than that asserted in Theorem 1. But the proof of Theorem 1 is simpler than that of Theorem 2, and provides a natural introduction to it.

2. Proof of Theorem 1. We defined $N(t)$ to be the number of times a particular combination of k digits occurs among the first t digits of a given decimal. More generally, we define $N(u, t)$ to be the number of times this combination occurs among the digits from the $(u+1)$th to the tth, so that $N(0, t) = N(t)$. This function is almost additive; we have, for $t > u$,

$$N(u, t) \leqq N(t) - N(u) \leqq N(u, t) + (k-1), \tag{2}$$

the discrepancy arising from the possibility that the combinations counted in $N(t) - N(u)$ may include some which contain both the uth and $(u+1)$th digits.

Let g be the degree of the polynomial $f(x)$. For any positive integer n, let x_n be the largest integer x for which $f(x)$ has less than n digits. Then, if n is sufficiently large, as we suppose throughout, $f(x_n + 1)$ has n digits, and so have $f(x_n + 2), \ldots, f(x_{n+1})$. It is obvious that

$$x_n \sim \mathfrak{a}(10^{1/g})^n \qquad \text{as } n \to \infty, \tag{3}$$

where $\mathfrak{a}$ is a constant.

Suppose that the last digit in $f(x_n)$ occupies the t_nth place in the decimal $\cdot f(1)f(2)\ldots$. Then the number of digits in the block

$$f(x_n + 1)f(x_n + 2)\ldots f(x_{n+1})$$

is $t_{n+1} - t_n$, and is also $n(x_{n+1} - x_n)$, since each f has exactly n digits. Hence

$$t_{n+1} - t_n = n(x_{n+1} - x_n). \tag{4}$$

It follows from (3) that

$$t_n \sim \mathfrak{a}n(10^{1/g})^n \qquad \text{as } n \to \infty. \tag{5}$$

To prove (1), it suffices to prove that

$$N(t_n, t) = 10^{-k}(t - t_n) + o(t_n) \tag{6}$$

as $n \to \infty$, for $t_n < t \leqq t_{n+1}$. For, by (2), we have

$$N(t) - N(t_h) = \sum_{r=h}^{n-1} N(t_r, t_{r+1}) + N(t_n, t) + R,$$

for a suitable fixed h, where $|R| < nk$. Since (6) includes as a special case the result

$$N(t_r, t_{r+1}) = 10^{-k}(t_{r+1} - t_r) + o(t_r),$$

we obtain (1).

In proving (6), we can suppose without loss of generality that t differs from t_n by an exact multiple of n. Putting $t = t_n + nX$, the number $N(t_n, t)$ is the number of times that the given combination of k digits occurs in the block

(7) $$f(x_n + 1)f(x_n + 2) \dots f(x_n + X),$$

where $0 < X \leqq x_{n+1} - x_n$. We can restrict ourselves to those combinations which occur entirely in the same $f(x)$, since the others number at most $(k - 1) \cdot (x_{n+1} - x_n)$, which is $o(t_n)$ by (3) and (5).

The number of times that a given combination $a_1a_2 \dots a_k$ of digits occurs in a particular $f(x)$ is the same as the number of values of m with $k \leqq m \leqq n$ for which the fractional part of $10^{-m}f(x)$ begins with the decimal $\cdot a_1a_2 \dots a_k$. If we define $\theta(z)$ to be 1 if z is congruent (mod 1) to a number lying in a certain interval of length 10^{-k}, and 0 otherwise, the number of times the given combination occurs in $f(x)$ is

$$\sum_{m=k}^{n} \theta(10^{-m}f(x)).$$

Hence

$$N(t_n, t) = \sum_{x=x_n+1}^{x_n+X} \sum_{m=k}^{n} \theta(10^{-m}f(x)) + O(x_{n+1} - x_n),$$

the error being simply that already mentioned.

To prove (6), it suffices to prove that

(8) $$\sum_{m=k}^{n} \sum_{x=x_n+1}^{x_n+X} \theta(10^{-m}f(x)) = 10^{-k}nX + o(n(x_{n+1} - x_n))$$

for $0 < X \leqq x_{n+1} - x_n$. We shall prove that if δ is any fixed positive number, and $\delta n < m < (1 - \delta)n$, then

(9) $$\sum_{x=x_n+1}^{x_n+X} \theta(10^{-m}f(x)) = 10^{-k}X + o(x_{n+1} - x_n)$$

uniformly in m. This suffices to prove (8), since the contribution of the remaining values of m is at most $2\delta nX$, where δ is arbitrarily small. We have

(10) $$X \leqq x_{n+1} - x_n < a(10^{1/\theta})^{n+1},$$

and we can also suppose that

(11) $$X > (x_{n+1} - x_n)^{1-\frac{1}{2}\delta} > \beta(10^{1/\theta})^{n(1-\frac{1}{2}\delta)},$$

where β is a constant, since (9) is trivial if this condition is not satisfied.

The proof of (9) follows well-known lines. One can construct [6; 4, pp. 91-92, 99] for any $\eta > 0$, functions $\theta_1(z)$ and $\theta_2(z)$, periodic in z with period 1, such that $\theta_1(z) \leqq \theta(z) \leqq \theta_2(z)$, having Fourier expansions of the form

$$\theta_1(z) = 10^{-k} - \eta + \sum_{\nu}' A_\nu^{(1)} e(\nu z),$$

$$\theta_2(z) = 10^{-k} + \eta + \sum_{\nu}' A_\nu^{(2)} e(\nu z).$$

Here the summation is over all integers ν with $\nu \neq 0$, and $e(w)$ stands for $e^{2\pi iw}$. The coefficients A_ν are majorized by

$$|A_\nu| \leqq \min\left(\frac{1}{|\nu|}, \frac{1}{\eta\nu^2}\right).$$

Using these functions to approximate $\theta(10^{-m}f(x))$ in (9), we see that it will suffice to estimate the sum

$$S_{n,m,\nu} = \sum_{x=x_n+1}^{x_n+X} e(10^{-m}\nu f(x)).$$

We can in fact prove that

$$|S_{n,m,\nu}| < CX^{1-\zeta} \tag{12}$$

for all m and ν satisfying

$$\delta n < m < (1-\delta)n, \qquad 1 \leqq \nu < \eta^{-2}, \tag{13}$$

where C and ζ are positive numbers depending only on δ, η and on the polynomial $f(x)$. This is amply sufficient to prove (9), since $X \leqq x_{n+1} - x_n$.

The inequality (12) is a special case of Weyl's inequality for exponential sums. The highest coefficient in the polynomial $10^{-m}\nu f(x)$ is $10^{-m}\nu c/d$, where c/d is the highest coefficient in $f(x)$, and so is a rational number. Write

$$10^{-m}\nu\frac{c}{d} = \frac{a}{q},$$

where a and q are relatively prime integers. Let $G = 2^{g-1}$. Then, by Weyl's inequality[1],

$$|S_{n,m,\nu}|^G < C_1X^\epsilon q^\epsilon(X^{G-1} + X^G q^{-1} + X^{G-g}q) \tag{14}$$

for any $\epsilon > 0$, where C_1 depends only on g and ϵ. In the present case, we have

$$q \leqq 10^m d < 10^{(1-\delta)n}d,$$

and

$$q \geqq 10^m\nu^{-1}c^{-1} > 10^{\delta n}\eta^2 c^{-1}.$$

This relates the magnitude of q to that of n. Relations between n and X were given in (10) and (11), and it follows that

$$C_2X^{g\delta} < q < C_3X^{g(1-\delta/3)},$$

where C_2 and C_3 depend only on η, c, d, and g. Using these inequalities for q in (14), we obtain a result of the form (12).

3. Proof of Theorem 2. We again consider the values of x for which $f(x)$ has exactly n digits, namely those for which $x_n < x \leqq x_{n+1}$. We denote by $T(x)$ the number of times that a particular digit combination $a_1a_2\ldots a_l$ (where $l \leqq k$) occurs in $f(x)$. Then, with the previous notation,

$$T(x) = \sum_{m=l}^{n} \theta(10^{-m}f(x)).$$

[1]The most accessible reference is [5, Satz 267]. The result is stated there for a polynomial with one term, but the proof applies generally.

We proved earlier that (putting $X = x_{n+1} - x_n$),

$$\sum_{x=x_n+1}^{x_n+X} T(x) \sim 10^{-l}nX \qquad \text{as } n \to \infty.$$

Now our object is a different one; we wish to estimate the number of values of x for which $T(x)$ deviates appreciably from its average value, which is $10^{-l}n$.

For this purpose, we shall prove that

$$\sum_{x=x_n+1}^{x_n+X} T^2(x) \sim 10^{-2l}n^2X \qquad \text{as } n \to \infty. \tag{15}$$

When this has been proved, Theorem 2 will follow. For then

$$\begin{aligned}\sum_{x=x_n+1}^{x_n+X} (T(x) - 10^{-l}n)^2 &= \Sigma T^2(x) - 2(10^{-l}n)\,\Sigma T(x) + 10^{-2l}n^2X \\ &= o(10^{-2l}n^2X) \qquad \text{as } n \to \infty.\end{aligned}$$

Hence the number of values of x with $x_n < x \leqq x_{n+1}$, for which the combination $a_1a_2 \ldots a_l$ does *not* occur between $(1 - \epsilon)10^{-l}n$ and $(1 + \epsilon)10^{-l}n$ times, is $o(x_{n+1} - x_n)$ for any fixed ϵ. Since this is true for each combination of at most k digits, it follows that $f(x)$ is (ϵ, k) normal for almost all x.

To prove (15), we write the sum on the left as

$$\sum_{x=x_n+1}^{x_n+X} \sum_{m_1=1}^{n} \sum_{m_2=1}^{n} \theta(10^{-m_1}f(x))\theta(10^{-m_2}f(x)). \tag{16}$$

Once again, we can restrict ourselves to values of m_1 and m_2 which satisfy

$$\delta n < m_1 < (1 - \delta)n, \quad \delta n < m_2 < (1 - \delta)n, \tag{17}$$

since the contribution of the remaining terms is small compared with the right hand side of (15) when δ is small. For a similar reason, we can impose the restriction that

$$m_2 - m_1 > \delta n. \tag{18}$$

Proceeding as before, and using the functions $\theta_1(z)$ and $\theta_2(z)$, we find that it suffices to estimate the sum

$$S(n, m_1, m_2, \nu_1, \nu_2) = \sum_{x=x_n+1}^{x_n+X} e((10^{-m_1}\nu_1 + 10^{-m_2}\nu_2)f(x)), \tag{19}$$

for values of ν_1 and ν_2 which are not both zero, and satisfy $|\nu_1| < \eta^{-2}$, $|\nu_2| < \eta^{-2}$. If either ν_1 or ν_2 is zero, the previous result (7) applies. Supposing neither zero, we write the highest coefficient again as

$$\left(10^{-m_1}\nu_1 + 10^{-m_2}\nu_2\right)\frac{c}{d} = \frac{a}{q}.$$

In view of (17) and (18), we have

$$q \leqq 10^{m_2}d < 10^{(1-\delta)n}d < C_3X^{(1-\delta)\theta}d.$$

We observe that a cannot be zero, since

$$10^{-m_2}|\nu_2| < 10^{-m_1-\delta n}|\nu_2| < \tfrac{1}{2}10^{-m_1}|\nu_1|,$$

provided that $2\eta^2 < 10^{\delta n}$, which is so for large n. Hence

$$q > \frac{2}{3}10^{m_1}|\nu_1|^{-1}c^{-1} > C_4X^{\delta\eta}.$$

It now follows as before from Weyl's inequality that

$$|S(n, m_1, m_2, \nu_1, \nu_2)| < CX^{1-\xi},$$

where again C and ξ are positive numbers depending only on δ, η, and the polynomial $f(x)$. Using this in (16), we obtain (15).

References

1. A. S. Besicovitch, *The asymptotic distribution of the numerals in the decimal representation of the squares of the natural numbers*, Math. Zeit., vol. 39 (1934), 146-156.
2. D. G. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc., vol. 8 (1933), 254-260.
3. A. H. Copeland and P. Erdös, *Note on normal numbers*, Bull. Amer. Math. Soc., vol. 52 (1946), 857-860.
4. J. F. Koksma, *Diophantische Approximationen* (Ergebnisse der Math., IV, 4; Berlin, 1936).
5. E. Landau, *Vorlesungen über Zahlentheorie* (Leipzig, 1927).
6. H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann., vol. 77 (1916), 313-352.

University College, London
The University, Aberdeen

ON PRODUCTS OF SETS OF GROUP ELEMENTS

HENRY B. MANN

LET $\mathfrak{A} = \{A_1, \ldots, A_s\}$, $\mathfrak{B} = \{B_1, \ldots, B_t\}$ be sets of elements of a group $\mathfrak{G}$ of finite order g. We define

$$\mathfrak{C} = \mathfrak{AB} = \{A_iB_j\}.$$

By $(\mathfrak{A})$, $(\mathfrak{B})$, ... we shall denote the number of elements in $\mathfrak{A}$, $\mathfrak{B}$, ... respectively and by $\overline{\mathfrak{A}}$, $\overline{\mathfrak{B}}$, ... the sets of elements of $\mathfrak{G}$ not in $\mathfrak{A}$,$\mathfrak{B}$, ...

THEOREM 1. *Either* $\mathfrak{AB} = \mathfrak{G}$ *or* $g \geqslant (\mathfrak{A}) + (\mathfrak{B})$.

Proof. Let $\overline{C}$ be an element not in $\mathfrak{C} = \mathfrak{AB}$. Let $A, B, \ldots$ be a generic notation for elements in $\mathfrak{A}, \mathfrak{B}, \ldots$ respectively. All A are different from all $\overline{C}B^{-1}$ for otherwise $\overline{C} = AB$. Thus there are at least $(\mathfrak{A}) + (\mathfrak{B})$ elements in $\mathfrak{G}$.

THEOREM 2. *Let* $\mathfrak{A}, \mathfrak{B}$ *be sets of elements of an Abelian group* $\mathfrak{G}$ *and let* $\overline{C} \subset \overline{\mathfrak{AB}}$. *Then there exists a* $\mathfrak{B}^* \supseteq \mathfrak{B}$ *such that*

(i) $\overline{\mathfrak{C}}^* = \overline{\mathfrak{A}\mathfrak{B}}^* = \mathfrak{H}\overline{C}$, *where* $\mathfrak{H}$ *is a subgroup of* $\mathfrak{G}$,

(ii) $(\mathfrak{AB}^*) - (\mathfrak{AB}) = (\mathfrak{B}^*) - (\mathfrak{B})$.

We shall give the proof by induction on the number of elements in $\overline{\mathfrak{C}}$. Clearly Theorem 2 holds with $\mathfrak{H} = I$ the identity if $\overline{\mathfrak{C}}$ consists only of one element $\overline{C}$. Now let $\overline{\mathfrak{C}}$ consist of the elements $\overline{C} = \overline{C}_0, \overline{C}_1, \ldots, \overline{C}_s$. Form the products $\overline{C}\,\overline{C}_i^{-1} = D_i$ and let $\mathfrak{H}$ be the subgroup generated by the D_i. Two cases arise.

First case. For every i and k we have for some m

$$\overline{C}_iD_k^{-1} = \overline{C}_m.$$

Since $\overline{C}_i = \overline{C}D_i^{-1}$ it then follows that for every $H \subset \mathfrak{H}$ we have for some m

$$\overline{C}H = \overline{C}_m.$$

Since $\overline{C}D_m^{-1} = \overline{C}_m$, so that $\overline{C}_m = \overline{C}H$ for every m, it follows that $\overline{\mathfrak{C}} = \overline{C}\mathfrak{H}$.

Second case. There exist an i and a k such that

$$\overline{C}_iD_k^{-1} = AE, \quad E \subset \mathfrak{B}.$$

We then form the set $\mathfrak{B}_1$ consisting of all elements of the form ED_j which satisfy an equation

$$AED_j = \overline{C}_t \tag{1}$$

Received August 2, 1950.

for some t. Equation (1) implies also

$$AED_t = \overline{C}_j. \tag{1'}$$

We shall prove:

PROPOSITION 1. *No element of* $\mathfrak{B}_1$ *is in* $\mathfrak{B}$. This follows easily since no element in $\mathfrak{B}$ can satisfy an equation of the form (1).

PROPOSITION 2. *Let* $\mathfrak{B} \cup \mathfrak{B}_1 = \mathfrak{B}_1^*$ *then* $\mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1^* \not\supset \overline{C}$. Otherwise we should have $AED_j = \overline{C}$, $AE = \overline{C}_j$ which is impossible since $E \subset \mathfrak{B}$ but $\overline{C}_j \not\subset \mathfrak{A}\mathfrak{B}$.

PROPOSITION 3. $(\mathfrak{A}\mathfrak{B}_1^*) - (\mathfrak{A}\mathfrak{B}) = (\mathfrak{B}_1^*) - (\mathfrak{B}) = (\mathfrak{B}_1)$.

Equations (1) and (1') show that ED_j is in $\mathfrak{B}_1$ if and only if $\overline{C}_j \subset \mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1^*$ which proves Proposition 3.

Since $(\overline{\mathfrak{C}}_1) < (\overline{\mathfrak{C}})$ there exists by induction a set $\mathfrak{B}^* \supset \mathfrak{B}_1^* \supset \mathfrak{B}$ such that $\overline{\mathfrak{A}\mathfrak{B}^*} = \overline{C}\mathfrak{H}$ where $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ and such that

$$(\mathfrak{A}\mathfrak{B}^*) - (\mathfrak{A}\mathfrak{B}_1^*) = (\mathfrak{B}^*) - (\mathfrak{B}_1^*).$$

Adding this equation to Proposition 3 we obtain Theorem 2.

COROLLARY (Davenport and Chowla). *Let* $\mathfrak{G}$ *be the additive group of residues* mod N. *Let* $\mathfrak{A} = \{a_0 = 0, a_1, \ldots, a_m\}$, $\mathfrak{B} = \{b_1, \ldots, b_n\}$ *be sets of residues* mod N *such that* $(a_i, N) = 1$ *for* $i > 0$. *Let* $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$. *Then either* $\mathfrak{C} = \mathfrak{G}$ *or*

$$(\mathfrak{C}) \geqslant m + n = (\mathfrak{A}) + (\mathfrak{B}) - 1. \tag{2}$$

Proof. By Theorems 1 and 2 it is sufficient to prove the Corollary for the case that $\overline{\mathfrak{C}} = \overline{C}\mathfrak{H}$ where $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$. Consider the factor group $\mathfrak{G}/\mathfrak{H}$. Let $\mathfrak{A}'$, $\mathfrak{B}'$ be the sets of cosets mod $\mathfrak{H}$ that contain elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Let t be the index and h the order of $\mathfrak{H}$. By Theorem 1,

$$t \geqslant (\mathfrak{A}') + (\mathfrak{B}').$$

Hence

$$N = ht \geqslant h(\mathfrak{A}') + h(\mathfrak{B}'). \tag{3}$$

Since $a_0 \subset \mathfrak{H}$, $a_i \not\subset \mathfrak{H}$ for $i > 0$, we have

$$h(\mathfrak{A}') - h \geqslant m, \quad h(\mathfrak{B}') \geqslant n.$$

Substituting this in (3) we obtain

$$N \geqslant m + n + h, \quad (\mathfrak{C}) = N - h \geqslant m + n.$$

The Corollary to Theorem 2 was proved by Davenport [2] for the case that N is a prime. Chowla [1] used Davenport's methods to obtain the Corollary in its general form. Davenport later discovered that for the case when N is a prime the Corollary was already known to Cauchy [3].

It is interesting to note that the proof of Theorem 2 is closely related to the author's proof of the fundamental theorem on the density of sums of sets of positive integers [4]. Thus the similarity between this theorem and the theorem of Davenport and Chowla is not as superficial as might have appeared.

References

1. I. Chowla, Proc. Indian Acad. Sci., vol. 2 (1935), 242-243.
2. H. Davenport, J. Lond. Math. Soc., vol. 10 (1935), 30-32.
3. ———, J. Lond. Math. Soc., vol. 22 (1947), 100-101.
4. H. B. Mann, Ann. of Math., vol. 43 (1942), 523-527.

Ohio State University

THE FOURIER COEFFICIENTS OF THE MODULAR FUNCTION $\lambda(\tau)$

WILLIAM H. SIMONS

1. Introduction. In [3], H. Rademacher obtained a convergent series for the Fourier coefficients of the modular invariant $J(\tau)$. He found that in the expansion

$$12^3 J(\tau) = e^{-2\pi i \tau} + \sum_{m=0}^{\infty} C_m e^{2\pi i m \tau}$$

the coefficients C_m, for $m \geqslant 1$, are given by

$$C_m = \frac{2\pi}{\sqrt{m}} \sum_{k=1}^{\infty} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right), \tag{1}$$

where

$$A_k(m) = \sum_{h \bmod k}{}' e^{-\frac{2\pi i}{k}(mh+h')}, \quad hh' \equiv -1 \pmod{k},$$

and $I_1(z)$ is the Bessel function of the first order with purely imaginary argument. The $\sum'$ above indicates the sum with respect to h from 0 to $k-1$ with $(h,k) = 1$. The purpose of this paper is to discuss the Fourier coefficients of $\lambda(\tau)$, the fundamental modular function of level (Stufe) 2. It may be defined either in terms of theta-functions by

$$\lambda(\tau) = \left[\frac{\theta_2(0|\tau)}{\theta_3(0|\tau)}\right]^4 = \left[\frac{\sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2}}{\sum_{n=-\infty}^{\infty} q^{n^2}}\right]^4 \tag{2}$$

$$= 16q \prod_{n=1}^{\infty} \left(\frac{1+q^{2n}}{1+q^{2n-1}}\right)^8 = 16q[1 - 8q + 44q^2 \ldots], \quad q = e^{\pi i \tau},$$

or by the equivalent definition

$$\lambda(\tau) = \kappa^2(\tau) = \frac{e_2 - e_3}{e_1 - e_3}, \tag{3}$$

where e_1, e_2, e_3 are given in terms of the Weierstrass elliptic function $\mathfrak{p}(z)$ and its periods $2\omega_1$, $2\omega_2$ by

$$e_1 = \mathfrak{p}(\omega_1), \quad e_2 = \mathfrak{p}(\omega_1 + \omega_2), \quad e_3 = \mathfrak{p}(\omega_2).$$

The function $\lambda(\tau)$ is invariant under the substitutions of the congruence subgroup $\Gamma(2)$ of the full modular group defined by all substitutions

Received August 25, 1950. This paper was prepared for publication while the author was a member of the Summer Research Institute of the Canadian Mathematical Congress.

$$\tau' = \frac{a\tau + b}{c\tau + d},$$

where a,b,c,d are integers with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2 \quad \text{and} \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1.$$

For the expansion

$$\lambda(\tau) = \sum_{m=0}^{\infty} a_m q^m, \quad q = e^{\pi i \tau},$$

it is found that

$$a_m = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{\infty} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right). \tag{4}$$

Moreover, it is found that the coefficients in the expansion of the reciprocal function

$$\mu(\tau) = \frac{1}{\lambda(\tau)} = \frac{1}{16q} + b_0 + \sum_{m=1}^{\infty} b_m e^{\pi i \tau m}$$

are given by the series

$$b_m = \frac{\pi}{8m^{\frac{1}{4}}} \sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{\infty} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right) \qquad (m > 1). \tag{5}$$

The method is essentially the same as that used by Rademacher. In §2 the transformation equations for $\lambda(\tau)$ are derived. The main result (4) is obtained in §§3 to 7, and equation (5) is derived in §8.

The following interesting comment was made by the referee of this paper. "The function $j(\tau)$ is determined essentially by its pole at $\tau = \infty$; it is regular everywhere else. But $1/j(\tau)$ has a pole at an interior point of the upper half-plane, and so *its* Fourier coefficients cannot be determined in as simple a manner. This situation is unavoidable with functions of the full modular group, which has but one parabolic cusp. On the other hand, the subgroup which Dr. Simons treats has 3 parabolic cusps, so it is possible to define functions which together with their reciprocals are regular in the upper half-plane by merely placing the zero and the pole at the cusps of the fundamental region. $\lambda(\tau)$ is such a function. It is of interest to note that both for $\lambda(\tau)$ and $1/\lambda(\tau)$, the Fourier coefficients are given by series which, apart from a trivial numerical factor, are composed of terms taken from the series for $j(\tau)$."

2. The transformation equations.

LEMMA 1. *Let a, b, c, d be integers with $ad - bc = 1$, and let*

$$\mathrm{T} = \frac{a\tau + b}{c\tau + d}.$$

Then $\lambda(T)$ *and* $\lambda(\tau)$ *are related as follows:*

	1°	2°	3°	4°	5°	6°
$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \pmod 2$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$
$\lambda(T)$	$\lambda(\tau)$	$\dfrac{\lambda(\tau)}{\lambda(\tau)-1}$	$\dfrac{1}{\lambda(\tau)}$	$\dfrac{1}{1-\lambda(\tau)}$	$1-\lambda(\tau)$	$1-\dfrac{1}{\lambda(\tau)}$

The lemma is an immediate consequence of the transformation equations for the theta-functions and definition (2), or of the transformation equations for e_1,e_2,e_3 and definition (3) [cf. 5].

LEMMA 2.

$$\lambda(2\tau) = \left[\frac{\{1-\lambda(\tau)\}^{\frac{1}{2}}-1}{\{1-\lambda(\tau)\}^{\frac{1}{2}}+1}\right]^2.$$

By definition,

$$\lambda(2\tau) = \frac{\theta_2^4(0|2\tau)}{\theta_3^4(0|2\tau)}.$$

But [5, p. 268],

$$2\theta_2^2(0|2\tau) = \theta_3^2(0|\tau) - \theta_4^2(0|\tau),$$

and

$$2\theta_3^2(0|2\tau) = \theta_3^2(0|\tau) + \theta_4^2(0|\tau),$$

where

$$\theta_4(0|\tau) = \sum_{n=-\infty}^{\infty}(-1)^n q^{n^2} = 1 - 2q + 2q^4 - \dots.$$

Therefore

$$\lambda(2\tau) = \frac{\theta_3^4 - 2\theta_3^2\theta_4^2 + \theta_4^4}{\theta_3^4 + 2\theta_3^2\theta_4^2 + \theta_4^4},$$

$$\frac{\lambda(2\tau)+1}{1-\lambda(2\tau)} = \frac{\theta_3^4+\theta_4^4}{2\theta_3^2\theta_4^2},$$

$$4\left[\frac{\lambda(2\tau)+1}{1-\lambda(2\tau)}\right]^2 = \frac{\theta_3^4}{\theta_4^4} + \frac{\theta_4^4}{\theta_3^4} + 2.$$

Now

$$\frac{\theta_4^4}{\theta_3^4} = \frac{\theta_3^4-\theta_2^4}{\theta_3^4} = 1 - \frac{\theta_2^4}{\theta_3^4} = 1 - \lambda(\tau),$$

and therefore

$$4\left[\frac{\lambda(2\tau)+1}{1-\lambda(2\tau)}\right]^2 = 1 - \lambda(\tau) + \frac{1}{1-\lambda(\tau)} + 2 = \frac{[2-\lambda(\tau)]^2}{1-\lambda(\tau)},$$

so that

$$\frac{\lambda(2\tau)+1}{1-\lambda(2\tau)} = \frac{2-\lambda(\tau)}{2\{1-\lambda(\tau)\}^{\frac{1}{2}}}.$$

Solving for $\lambda(2\tau)$ gives

$$\lambda(2\tau) = \frac{\dfrac{2-\lambda(\tau)}{2\{1-\lambda(\tau)\}^{\frac{1}{2}}} - 1}{\dfrac{2-\lambda(\tau)}{2\{1-\lambda(\tau)\}^{\frac{1}{2}}} + 1}$$

$$= \frac{2-\lambda(\tau)-2\{1-\lambda(\tau)\}^{\frac{1}{2}}}{2-\lambda(\tau)+2\{1-\lambda(\tau)\}^{\frac{1}{2}}}$$

$$= \left[\frac{\{1-\lambda(\tau)\}^{\frac{1}{4}}-1}{\{1-\lambda(\tau)\}^{\frac{1}{4}}+1}\right]^2.$$

THEOREM 2. *Let k be an even integer and h and h' be integers such that $(h, k) = 1$, and $hh' \equiv -1 \pmod{k}$. Further, let*

$$\tau = 2\left(\frac{h}{k} + \frac{iz}{k}\right) \text{ and } \mathrm{T} = 2\left(\frac{h'}{k} + \frac{i}{kz}\right).$$

Then

$$\lambda(\mathrm{T}) = \begin{cases} \lambda(\tau) & \text{if } k \equiv 0 \pmod 4, \\ 1/\lambda(\tau) & \text{if } k \equiv 2 \pmod 4. \end{cases}$$

Proof. Define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} h' & 2(-1-hh')/k \\ k/2 & -h \end{pmatrix}.$$

Then a, b, c, d are integers with $ad - bc = 1$, and

$$\mathrm{T} = \frac{a\tau + b}{c\tau + d}$$

If $k \equiv 0 \pmod 4$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

and so by Lemma 1, case 1°, $\lambda(\mathrm{T}) = \lambda(\tau)$. If $k \equiv 2 \pmod 4$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod 2$$

and so by Lemma 1, case 3°, $\lambda(\mathrm{T}) = 1/\lambda(\tau)$.

THEOREM 2. *Let k be an odd integer and let h and h' be integers such that $(h,k) = 1$ and $hh' \equiv -1 \pmod{k}$.*
Further, let

$$\tau = \left(\frac{h}{k} + \frac{iz}{k}\right), \quad \mathrm{T} = \left(\frac{h'}{k} + \frac{i}{kz}\right).$$

Then

$$\lambda(2\tau) = \begin{cases} [\{\lambda(\mathrm{T})-1\}^{\frac{1}{4}} - \lambda(\mathrm{T})]^4, & \text{if } h \equiv 1 \pmod 2, \\ \left[\dfrac{\{\lambda(\mathrm{T})\}^{\frac{1}{4}}-1}{\{\lambda(\mathrm{T})\}^{\frac{1}{4}}+1}\right]^2, & \text{if } h \equiv 0 \pmod 2. \end{cases}$$

Proof. Define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} h' & (-1-hh')/k \\ k & -h \end{pmatrix}.$$

Then a, b, c, d are integers with $ad - bc = 1$ and

$$T = \frac{a\tau + b}{c\tau + d}.$$

(a). Let $h' \equiv 1 \pmod 2$ and $h \equiv 1 \pmod 2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod 2,$$

and so by Lemma 1, case 3°, $\lambda(T) = 1/\lambda(\tau)$. Substituting for $\lambda(\tau)$ in Lemma 2 gives

$$\lambda(2\tau) = \left[\frac{\{1 - 1/\lambda(T)\}^{\frac{1}{4}} - 1}{\{1 - 1/\lambda(T)\}^{\frac{1}{4}} + 1}\right]^2 = \left[\frac{\{\lambda(T) - 1\}^{\frac{1}{4}} - \{\lambda(T)\}^{\frac{1}{4}}}{\{\lambda(T) - 1\}^{\frac{1}{4}} + \{\lambda(T)\}^{\frac{1}{4}}}\right]^2.$$

(b). Let $h' \equiv 1 \pmod 2$ and $h \equiv 0 \pmod 2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2,$$

and so by Lemma 1, case 6°, $\lambda(\tau) = 1/(1 - \lambda(T))$. Substituting for $\lambda(\tau)$ in Lemma 2 gives

$$\lambda(2\tau) = \left[\frac{\left\{\dfrac{\lambda(T)}{\lambda(T) - 1}\right\}^{\frac{1}{4}} - 1}{\left\{\dfrac{\lambda(T)}{\lambda(T) - 1}\right\}^{\frac{1}{4}} + 1}\right]^2 = \left[\frac{\{\lambda(T)\}^{\frac{1}{4}} - \{\lambda(T) - 1\}^{\frac{1}{4}}}{\{\lambda(T)\}^{\frac{1}{4}} + \{\lambda(T) - 1\}^{\frac{1}{4}}}\right]^2.$$

(c). Let $h' \equiv 0 \pmod 2$ and $h \equiv 1 \pmod 2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2$$

and so by Lemma 1, case 4°, $\lambda(\tau) = 1 - 1/\lambda(T)$. Substituting in Lemma 2 gives

$$\lambda(2\tau) = \left[\frac{\{\lambda(T)\}^{-\frac{1}{4}} - 1}{\{\lambda(T)\}^{-\frac{1}{4}} + 1}\right]^2 = \left[\frac{\{\lambda(T)\}^{\frac{1}{4}} - 1}{\{\lambda(T)\}^{\frac{1}{4}} + 1}\right]^2.$$

(d). Let $h' \equiv 0 \pmod 2$ and $h \equiv 0 \pmod 2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2$$

and so by Lemma 1, case 5°, $\lambda(\tau) = 1 - \lambda(T)$. Substituting in Lemma 2 then gives

$$\lambda(2\tau) = \left[\frac{\{\lambda(T)\}^{\frac{1}{4}} - 1}{\{\lambda(T)\}^{\frac{1}{4}} + 1}\right]^2.$$

By combining the results of (a) with (b) and those of (c) with (d) the result of the theorem is obtained.

3. The Farey dissection. Let

$$\lambda(\tau) = f(q) = \sum_{m=1}^{\infty} a_m q^m, \qquad q = e^{\pi i \tau}.$$

Then by Cauchy's theorem,

$$a_m = \frac{1}{2\pi i}\int_C \frac{f(q)}{q^{m+1}}\, dq,$$

where the integration is in the positive sense around the circle C defined by

$$|q| = e^{-2\pi N^{-2}},$$

N being a positive integer. Using the Farey dissection of order N of the circle C, the integral may be expressed by the sum

$$a_m = \frac{1}{2\pi i} \sum_{\substack{0 \leqq h < k \leqq N \\ (h,k)=1}} \int_{\xi_{h,k}} \frac{f(q)}{q^{m+1}}\, dq,$$

where $\xi_{h,k}$ is the Farey arc corresponding to the fraction h/k in the Farey series of order N, and

$$q = \exp\left(-2\pi N^{-2} + 2\pi i \frac{h}{k} + 2\pi i \phi\right).$$

Then

$$a_m = \sum_{\substack{0 \leqq h < k \leqq N \\ (h,k)=1}} \int_{-\phi'}^{\phi''} \frac{f\left(\exp\left\{-2\pi N^{-2} + 2\pi i \frac{h}{k} + 2\pi i \phi\right\}\right)}{\exp\left(-2\pi m N^{-2} + 2\pi i m \frac{h}{k} + 2\pi i m \phi\right)}\, d\phi,$$

where

$$\begin{aligned} \phi' &= \frac{h}{k} - \frac{h+h_1}{k+k_1} = \frac{1}{k(k+k_1)}, \\ \phi'' &= \frac{h+h_2}{k+k_2} - \frac{h}{k} = \frac{1}{k(k+k_2)}, \end{aligned} \tag{6}$$

h_1/k_1, h/k, h_2/k_2 being three consecutive terms of the Farey series of order N. For convenience the double sum over $0 \leqq h < k \leqq N$ with $(h,k) = 1$ will be denoted by

$$\sum_{h,k}^{N}.$$

Then

$$a_m = \exp(2\pi m N^{-2}) \sum_{h,k}^{N} \exp\left(-2\pi i m \frac{h}{k}\right) \cdot \int_{-\phi'}^{\phi''} f\left(\exp\left\{-2\pi N^{-2} + 2\pi i \frac{h}{k} + 2\pi i \phi\right\}\right) \exp(-2\pi i m \phi)\, d\phi$$

$$= \exp(2\pi mN^{-2}) \sum_{h,k}^{N} \exp\left(-2\pi i m \frac{h}{k}\right)$$
$$\cdot \int_{-\phi'}^{\phi''} f\left(\exp\left\{2\pi i\left(\frac{h}{k} + \frac{iz}{k}\right)\right\}\right) \exp(-2\pi i m\phi) d\phi,$$

where $z = k(N^{-2} - i\phi)$.

Now let the above summation be broken up into three sums Σ_1, Σ_2, Σ_3, the first consisting of those terms for which $k \equiv 1 \pmod 2$, the second those for which $k \equiv 2 \pmod 4$, and the third those for which $k \equiv 0 \pmod 4$, and let I_1, I_2, and I_3, be the parts of a_m corresponding to Σ_1, Σ_2, Σ_3 respectively. Thus

$$a_m = I_1 + I_2 + I_3.$$

4. Evaluation of the integral I_3.

$$I_3 = \exp(2\pi mN^{-2}) \sum_{k=0 \pmod 4}^{N} \sum_{(h,k)=1}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right)$$
$$\cdot \int_{-\phi'}^{\phi''} f\left(\exp\left\{2\pi i\left(\frac{h}{k} + \frac{iz}{k}\right)\right\}\right) \exp(-2\pi i m\phi) d\phi.$$

Applying the transformation equation of Theorem 1, for $k \equiv 0 \pmod 4$ gives

$$I_3 = \exp(-2\pi mN^{-2}) \sum_{k=0 \pmod 4}^{N} \sum_{(h,k)=1}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right)$$
$$\cdot \int_{-\phi'}^{\phi''} f\left(\exp\left\{2\pi i\left(\frac{h'}{k} + \frac{i}{kz}\right)\right\}\right) \exp(-2\pi i m\phi) d\phi.$$

But

$$f(q) = \lambda(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = \exp \pi i \tau,$$

and so, substituting for $f(q)$, rearranging terms, and putting $\omega = N^{-2} - i\phi$, $z = k\omega$, gives

$$I_3 = \sum_{k=0 \pmod 4}^{N} \sum_{(h,k)=1}^{k-1} \int_{-\phi'}^{\phi''} \sum_{n=1}^{\infty} a_n \exp\left\{\frac{2\pi i}{k}(nh' - mh)\right\} \exp\left(2\pi m\omega - \frac{2\pi n}{k^2\omega}\right) d\phi.$$

Use is now made of a result due to Estermann [2]. Let ϕ' and ϕ'' be defined by (6), and let

$$g(N, \phi, h, k) = \begin{cases} 1, & \text{for } -\phi' < \phi < \phi'', \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$g = \sum_{r=1}^{k} b_r \exp\{2\pi i r h'/k\},$$

where h' is an integer satisfying $hh' \equiv -1 \pmod k$, and b_r is independent of h and

$$\sum_{r=1}^{k} |b_r| < \log 4k.$$

Introducing the function $g(N,\phi,h,k)$ into the integral I_3 gives

$$I_3 = \sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{N} \sum_{n=1}^{\infty} a_n \int_{-1/k(N+1)}^{1/k(N+1)} \sum_{r=1}^{k} b_r \exp\left(2\pi i r \frac{h'}{k}\right) \cdot \exp\left(2\pi m\omega - \frac{2\pi n}{k^2\omega}\right) \sum_{h \bmod k}{}' \exp\left\{\frac{2\pi i}{k}(nh' - mh)\right\} d\phi.$$

The latter sum is a Kloosterman sum [4;1] and has the estimate $O(k^{2/3+\epsilon}m^{1/3})$. Also, the real part of $2\pi n/k^2\omega$ is

$$\Re\left(\frac{2\pi n}{k^2(N^{-2} - i\phi)}\right) = \frac{2\pi n N^{-2}}{k^2(N^{-4} + \phi^2)} > \frac{2\pi n}{k^2N^{-2} + k^2N^2\phi''^2}$$

$$> \frac{2\pi n}{1+1} = \pi n,$$

and

$$\Re(2\pi m\omega) = 2\pi m N^{-2}.$$

Therefore

$$|I_3| = O\left(\sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{N} \sum_{n=1}^{\infty} a_n e^{-\pi n} \int_{-1/k(N+1)}^{1/k(N+1)} \sum_{r=1}^{k} |b_r| \exp\,(2\pi m N^{-2}) k^{2/3+\epsilon} m^{1/3} d\phi\right)$$

$$= O\left(\sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{N} m^{1/3} k^{2/3+\epsilon} \log 4k \int_{-1/k(N+1)}^{1/k(N+1)} d\phi\right)$$

$$= O\left(\sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{N} m^{1/3} k^{2/3+\epsilon} \frac{1}{kN}\right)$$

and so

$$|I_3| = O\left(N^{-1} \sum_{k=1}^{N} k^{-1/3+\epsilon} m^{1/3}\right)$$

$$= O\left(N^{-1/3+\epsilon} m^{1/3}\right).$$

5. Evaluation of the integral I_2.

$$I_2 = \exp\,(2\pi m N^{-2}) \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right) \cdot \int_{-\phi'}^{\phi''} f\left(\exp\left\{2\pi i\left(\frac{h}{k} + \frac{iz}{k}\right)\right\}\right) \exp\,(-2\pi i m\phi) d\phi.$$

Now, by Theorem 1, with $k \equiv 2 \pmod 4$, and putting $q = e^{\pi i \tau}$ and $q' = e^{\pi i \Gamma}$,

$$f(q) = \lambda(\tau) = \frac{1}{\lambda(T)} = f_1(q') = \left[\frac{\theta_3(0|T)}{\theta_2(0|T)}\right]^4$$

$$= \frac{1}{16q'} + \sum_{n=0}^{\infty} b_n q'^n$$

$$= \frac{1}{16q'} + f_2(q').$$

Therefore

$$I_2 = \exp(2\pi mN^{-2}) \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right)$$

$$\cdot \int_{-\phi'}^{\phi''} f_1\left(\exp\left\{2\pi i\left(\frac{h'}{k} + \frac{i}{kz}\right)\right\}\right) \exp(-2\pi i m\phi) d\phi$$

$$= I_{2,1} + I_{2,2},$$

where $f_1(q')$ is replaced by $1/16q'$ in $I_{2,1}$ and by $f_2(q')$ in $I_{2,2}$. Introducing the function $g(N,\phi,h,k)$ into the integral $I_{2,2}$ and proceeding as in §4 gives

$$|I_{2,2}| = O\left(\sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} \sum_{n=0}^{\infty} b_n e^{-\pi n} \int_{-1/k(N+1)}^{1/k(N+1)} \sum_{r=1}^{k} |b_r| \exp(2\pi mN^{-2}) k^{2/3+\epsilon} m^{1/3} d\phi\right)$$

$$= O\left(\frac{1}{N} \sum_{k=1}^{N} k^{2/3+\epsilon} m^{1/3}\right)$$

$$= O(N^{-1/3+\epsilon} m^{1/3}).$$

Next,

$$I_{2,1} = \exp(2\pi mN^{-2}) \sum_{k=2 \pmod 4}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right)$$

$$\cdot \int_{-\phi'}^{\phi''} \frac{1}{16} \exp\left(-2\pi i\left\{\frac{h'}{k} + \frac{i}{kz}\right\}\right) \exp(-2\pi i m\phi) d\phi$$

$$= \frac{1}{16} \sum_{k=2 \pmod 4}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-\frac{2\pi i}{k}\left\{mh + h'\right\}\right)$$

$$\cdot \int_{-\phi'}^{\phi''} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right) d\phi$$

$$= \frac{i}{16} \sum_{k=2 \pmod 4}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-\frac{2\pi i}{k}\left\{mh + h'\right\}\right)$$

$$\cdot \int_{N^{-2}-i\omega''}^{N^{-2}+i\omega'} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right) d\omega.$$

Now,

$$\phi' = \frac{1}{k(k_1+k)} < \frac{1}{k(N+1)}$$

and

$$\phi'' = \frac{1}{k(k_2+k)} < \frac{1}{k(N+1)},$$

and so

$$I_{2,1} = -\frac{1}{16} \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-\frac{2\pi i}{k}\{mh+h'\}\right)$$
$$\cdot \left[\int^{(0+)} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)d\omega - \left\{\int_{N^{-2}+\omega'}^{N^{-2}+1/k(N+1)} + \int_{N^{-2}+1/k(N+1)}^{-N^{-2}+1/k(N+1)} + \int_{-N^{-2}+1/k(N+1)}^{-N^{-2}-1/k(N+1)} + \int_{-N^{-2}-1/k(N+1)}^{N^{-2}-1/k(N+1)} + \int_{N^{-2}-1/k(N+1)}^{N^{-2}-\omega''}\right\} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)d\omega\right]$$

$$= \frac{\pi}{8} \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} A_k(m) \frac{1}{2\pi i} \int^{(0+)} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)d\omega \tag{7}$$
$$+ K_1 + K_2 + K_3 + K_4 + K_5,$$

where

$$A_k(m) = \sum_{h \bmod k} \exp\left(-\frac{2\pi i}{k}\{mh+h'\}\right).$$

Now

$$K_1 = \frac{i}{16} \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{N} A_k(m) \int_{N^{-2}+i/k(N+1)}^{N^{-2}+i/k} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)d\omega.$$

Introducing the function $g(N,\phi,h,k)$, and integrating from $N^{-2}+ i/k(N+k)$ to $N^{-2}+ i/k(N+1)$ gives

$$|K_1| = O\left(\sum_{k=1}^{N} k^{3/2+\epsilon} m^{1/2} \log 4k \frac{1}{kN}\right) = O(N^{-1/2+\epsilon} m^{1/2}).$$

Similarly

$$|K_5| = O(N^{-1/2+\epsilon} m^{1/2}).$$

In K_2,

$$\omega = u + i/k(N+1), \quad -N^{-2} \leqslant u \leqslant N^{-2},$$

$$\Re\left(\frac{1}{\omega}\right) = \frac{u}{u^2 + 1/k^2(N+1)^2} < N^{-2}k^2(N+1)^2 < k^2,$$

so that

$$\left|\exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)\right| < \exp\left(2\pi m N^{-2} + 2\pi\right).$$

Therefore

$$|K_2| = O\left(\sum_{k=1}^{N} k^{2/3+\epsilon} m^{1/3} N^{-2}\right) = O(N^{-1/3+\epsilon} m^{1/3}).$$

Similarly

$$|K_4| = O(N^{-1/3+\epsilon} m^{1/3}).$$

Again, in K_3,

$$\omega = -N^{-2} + iv, \quad -\frac{1}{k(N+1)} \leqslant v \leqslant \frac{1}{k(N+1)}.$$

Also

$$\Re(\omega) = -N^{-2} < 0$$

$$\Re\left(\frac{1}{\omega}\right) = \Re\left(\frac{1}{-N^{-2}+iv}\right) = \frac{-N^{-2}}{N^{-4}+v^2} < 0,$$

and hence

$$\left|\exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right)\right| < 1.$$

Therefore

$$|K_3| = O\left(\sum_{k=1}^{N} k^{2/3+\epsilon} m^{1/3} \frac{1}{kN}\right) = O(N^{-1/3+\epsilon} m^{1/3}).$$

Collecting these results together and substituting back into (7) gives

$$I_{2,1} = \frac{\pi}{8} \sum_{\substack{k=1 \\ k=2 \pmod 4}}^{N} A_k(m) L_k(m) + O(N^{-1/3+\epsilon} m^{1/3}),$$

where [6; 3]

$$L_k(m) = \frac{1}{2\pi i}\int^{(0+)} \exp\left(2\pi m\omega + \frac{2\pi}{k^2\omega}\right) d\omega = \frac{1}{k\sqrt{m}} I_1\left(\frac{4\pi\sqrt{m}}{k}\right),$$

$I_1(z)$ being the Bessel function of the first order with purely imaginary argument. Therefore

$$I_2 = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k=2 \pmod 4}}^{N} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right) + O(N^{-1/3+\epsilon} m^{1/3}).$$

6. Evaluation of the integral I_1. In I_1, consider

$$\tau = \frac{h}{k} + \frac{iz}{k}, \quad \mathrm{T} = \frac{h'}{k} + \frac{i}{kz}$$

so that

$$f\left(\exp\left\{2\pi i\left(\frac{h}{k} + \frac{iz}{k}\right)\right\}\right) = f(\exp\{2\pi i\tau\}) = \lambda(2\tau).$$

Then, by Theorem 2, with $t = \exp \pi i \mathrm{T}$,

$$\lambda(2\tau) = 1 + 16it^{\frac{1}{2}} - 128t + \ldots$$

when $h' \equiv 1 \pmod 2$, and

$$\lambda(2\tau) = 1 - 16t^{\frac{1}{2}} + 128t - \ldots$$

when $h' \equiv 0 \pmod 2$. These may be combined by replacing t by $t' = \exp \pi i(T + h') = t \exp(\pi i h')$, giving

$$\lambda(2\tau) = 1 + 16t'^{\frac{1}{2}} + 128t' + \ldots = \sum_{n=0}^{\infty} u_n t'^{\frac{1}{2}n}.$$

Applying the transformations of Theorem 2 to the integrand of I_1 gives

$$I_1 = \exp(2\pi m N^{-2}) \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2}}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right) \cdot \int_{-\phi'}^{\phi''} \sum_{n=0}^{\infty} u_n \exp\left\{\frac{\pi i n}{2}\left(\frac{h'}{k} + \frac{i}{kz}\right)\right\} \exp\left(\frac{\pi i n h'}{2}\right) \exp(-2\pi i m\phi) d\phi$$

$$= \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2}}^{N} \sum_{n=0}^{\infty} (-1)^{nh'/2} \int_{-1/k(N+1)}^{1/k(N+1)} \sum_{r=1}^{k} b_r \exp\left(2\pi i r \frac{h'}{k}\right) \cdot \exp\left(2\pi m\omega - \frac{\pi n}{2k^2\omega}\right) \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left\{\frac{\pi i}{2k}(nh' - 4mh)\right\} d\phi.$$

Now the latter sum in the integrand is an incomplete Kloosterman sum for which we have [2; 4] the estimate

$$O(k^{2/3+\epsilon}(4m, k)^{1/3}) = O(k^{2/3+\epsilon} m^{1/3}).$$

Also

$$\Re\left(\frac{\pi n}{2k^2\omega}\right) = \frac{\pi n N^{-2}}{2(k^2 N^{-2} + k^2 N^2 \phi''^2)} > \frac{\pi n}{4}.$$

Therefore

$$|I_1| = O\left(\sum_{k=1}^{N} k^{2/3+\epsilon} m^{1/3} \sum_{n=0}^{\infty} |u_n| e^{-\pi n/4} \exp 2\pi m N^{-2} \int_{-1/k(N+1)}^{1/k(N+1)} d\phi\right)$$

$$= O\left(\frac{1}{N} \sum_{k=1}^{N} k^{-1/3+\epsilon} m^{1/3}\right)$$

$$= O(N^{-1/3+\epsilon} m^{1/3}).$$

7. The convergent series for a_m. Collecting together the results of §§4, 5, and 6, we have

$$a_m = I_1 + I_2 + I_3 = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k \equiv 2 \pmod 4}}^{N} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right) + O(N^{-1/3+\epsilon} m^{1/3}).$$

Finally, letting $N \to \infty$, we get

$$a_m = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k \equiv 2 \pmod 4}}^{\infty} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right). \tag{4}$$

As a numerical example we may compare the actual value of a_{16} with the value obtained from the series (4). Thus $a_{16} = -316342272$. Using the series for a_{16}, we have

$$a_{16} = \frac{\pi}{32} \sum_{\substack{k=1 \\ k\equiv 2 \pmod 4}}^{\infty} \frac{A_k(16)}{k} I_1\left(\frac{16\pi}{k}\right),$$

$$\frac{\pi}{64} A_2(16) I_1\left(\frac{16\pi}{2}\right) = -316342253.1678$$

$$\frac{\pi}{192} A_6(16) I_1\left(\frac{16\pi}{6}\right) = -18.6991$$

$$\frac{\pi}{320} A_{10}(16) I_1\left(\frac{16\pi}{10}\right) = -0.0935.$$

8. The reciprocal function $\mu(\tau)$.

THEOREM 3. *Let*

$$\mu(\tau) = g(q) = \frac{1}{\lambda(\tau)} = \left[\frac{\theta_3(0|\tau)}{\theta_2(0|\tau)}\right]^4$$

$$= \frac{1}{16q}(1 + 8q + 20q^2 + \ldots)$$

$$= \frac{1}{16q} + \sum_{m=0}^{\infty} b_m q^m.$$

Then, for $m > 0$,

$$b_m = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{\infty} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right). \tag{5}$$

Proof. Since the analysis in this case is essentially the same as for $\lambda(\tau)$, we will only outline the proof. The transformation equations for $\mu(\tau)$ may be obtained directly from those for $\lambda(\tau)$. Now, by Cauchy's theorem, for $m > 0$,

$$b_m = \frac{1}{2\pi i}\int_C \frac{g(q)}{q^{m+1}} dq,$$

where, as before, C is the circle of radius $|q| = \exp(-2\pi N^{-2})$. Therefore

$$b_m = \exp(2\pi m N^{-2}) \sum_{k=1}^{N} \sum_{\substack{h=0 \\ (h,k)=1}}^{k-1} \exp\left(-2\pi i m \frac{h}{k}\right)$$

$$\cdot \int_{-\phi'}^{\phi''} g\left(\exp\left\{2\pi i\left(\frac{h}{k} + \frac{iz}{k}\right)\right\}\right) \exp(-2\pi i m\phi) d\phi.$$

Let $b_m = b_{m,1} + b_{m,2} + b_{m,3}$, where $b_{m,1}$ consists of the terms of b_m for which $k \equiv 1 \pmod 2$, $b_{m,2}$ those for which $k \equiv 2 \pmod 4$, and $b_{m,3}$ those for which $k \equiv 0 \pmod 4$. Then it may be shown that

$$b_{m,1} = O(N^{-1/3+\epsilon}m^{1/3}), \quad b_{m,2} = O(N^{-1/3+\epsilon}m^{1/3})$$

and

$$b_{m,3} = \frac{\pi}{8\sqrt{m}} \sum_{\substack{k=1 \\ k\equiv 0 \pmod 4}}^{N} \frac{A_k(m)}{k} I_1\left(\frac{4\pi\sqrt{m}}{k}\right) + O(N^{-1/3+\epsilon}m^{1/3}).$$

Then letting $N \to \infty$ we get equation (5).

Similar results may be obtained for the Fourier coefficients of powers of $\lambda(\tau)$ and $\mu(\tau)$. However, these are omitted here since the method used in obtaining them is merely a repetition of that given for $\lambda(\tau)$.

References

1. H. Davenport, *On certain exponential sums*, J. Reine Angew. Math., Bd. 169 (1933), 158-176.
2. T. Estermann, *Vereinfachter Beweis eines Satz von Kloosterman*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, Bd. 7 (1939), 82-98, especially 94.
3. H. Rademacher, *The Fourier coefficients of the modular invariant $J(\tau)$*, Amer. J. Math., vol. 60 (1938), 501-512.
4. H. Salié, *Zur Abschatzung der Fourierkoeffizienten ganzer Modulformen*, Math. Z., Bd. 36 (1933), 263-278.
5. J. Tannery and J. Molk, *Théorie des fonctions elliptiques*, Tome II (Paris, 1896), 290.
6. G. N. Watson, *Theory of Bessel functions* (Cambridge, 1922), 181.

The University of British Columbia

AXIOMS FOR ELLIPTIC GEOMETRY

DAVID GANS

Introduction. Until recently the literature contained little on the axiomatic foundations of elliptic geometry that was non-analytical and independent of projective geometry. During the past decade this subject has come in for further study, notably by Busemann [2] and Blumenthal [1], who supplied such foundations. This paper presents another and, it is believed, simpler effort in the same general direction, proceeding by the familiar synthetic methods of elementary geometry and using only elementary topological notions and ideas concerning metric spaces. Specifically, elliptic 2-space is obtained on the basis of six axioms, most notable of which is one assuming the existence of translations. The writer wishes to express his deep appreciation to Herbert Busemann for his invaluable help.

I. Some basic terms and notations

Small letters always denote points. The *distance* between two points a,b of any metric space is denoted by ab or ba. A point c is said to be *between* points a,b (denoted by acb or bca) if $c \neq a$ or b and $ac + cb = ab$, and is said to be a *midpoint* of a and b (denoted by $c = \text{mid}(a,b)$) if, moreover, $ac = cb$. An *arc*, a *simple arc*, and a *geodesic arc* mean, respectively, a continuous, a topological, and a congruent map of a closed Euclidean segment; a simple closed curve means the homeomorph of a Euclidean circle. An arc or geodesic arc with endpoints a,b is said to *lie between* a and b, and is denoted by (ab) or $[ab]$, respectively. When no confusion can arise "geodesic arc" is often shortened to "arc", as in the phrase "the arc $[ab]$". In the interest of clarity of presentation and ease of reference, as well as to offer brief proofs, the number of theorems used has been large. Each theorem, when first stated, is denoted merely by an Arabic numeral, the word "Theorem" being omitted. Some proofs are not given.

II. Geodesic arcs and straight lines

Axiom 1. Σ is a compact metric space with at least two points.

Σ is then bounded, and the function xy, where x and y are arbitrary points of Σ, has a maximum. We take this maximum as unit distance, calling points a and b *conjugate* if $ab = 1$.

Axiom 2. Any distinct points a,b have just one midpoint if non-conjugate, just two if conjugate.

1. *If abc, then a and b have a unique midpoint, and likewise for b and c.*

Received September 23, 1950; in revised form September 17, 1951.

Σ is *convex* by Axiom 2, i.e., there is a point between each two points. From Menger [4] we then infer Theorems 2 to 4; Theorem 5 is immediate; Theorem 6 follows from Theorem 1, Menger [4], and Axiom 1.

2. *There exists a geodesic arc between any two distinct points.*

3. *An arc (ab) is a geodesic arc if and only if its length equals ab, or if it is the shortest arc between a and b.*

4. *The geodesic arcs $[ab]$ are distinguished among all the arcs (ab) by the property that if p,q are inner points of $[ab]$, then apq or qpb or $p = q$.*

5. *If p is an inner point of $[ab]$, then apb.*

6. *There is just one geodesic arc between two non-conjugate points, just two between two conjugate points.*

7. *If $ab = 1$ the two geodesic arcs $[ab]$ have only a and b in common.*

8. *If p,q are inner points of $[ab]$, and apq, then pqb.*

9. *If abc, then there is only one arc $[ab]$ and one arc $[bc]$, $[ab] + [bc]$ is an arc $[ac]$, and b is an inner point of an arc $[ac]$.*

AXIOM 3a. If abc and abd, then either $c = d$ or bcd or cbd.

b. If abc and bcd, where $ab + bc + cd < 1$, then abd.

AXIOM 4. If c is a midpoint of a and b, then a point d exists such that $cd = 1$, cad, and cbd.

10. *If abc and abd, then either $c = d$; or acd, bcd; or adc, bdc.*

Proof. Menger showed that abc, abd, acd imply bcd [4, p. 107]. Similarly one can easily show that abc, abd, bcd imply acd. Now assume abc and abd. Then either $c = d$ or bcd or bdc by Axiom 3a. If bcd, then acd by the proposition stated two sentences back. If bdc, then adc, as can be seen by interchanging c and d in the proposition stated in the first sentence.

11. *The point d described in Axiom 4 is unique.*

Proof. Assume d' is another point having the same properties as d. Then $cd' = 1$, cad', and cbd'. Since cad and cad' we infer by Theorem 10 that either $d = d'$; or cdd', add'; or $cd'd$, $ad'd$. Now cdd' means that $cd + dd' = cd'$, where c,d,d' are all distinct, and this is impossible since $cd = cd' = 1$. Likewise $cd'd$ is impossible. Hence $d = d'$.

DEFINITION 1. Let a,b be any distinct points, $c = \text{mid}(a,b)$, and d the unique point such that $cd = 1$, cad, and cbd. The point-set consisting of c, d, and all points between c and d is called a *straight line* (or *line*) determined by a and b.

12. *A unique straight line is determined by any two distinct points a and b, this straight line being denoted by $-ab-$. Every straight line is a simple closed curve of length 2.*

Proof. If $ab < 1$, a and b have a unique midpoint c and hence determine a unique line. If d is the point such that $cd = 1$, cad, and cbd, it follows from Theorems 7 and 9 that this line is the simple closed curve of length 2 formed by the two arcs $[cd]$. If $ab = 1$, let $c' = \text{mid}(a,b)$ and d' be the point such that $c'd' = 1$, $c'ad'$, and $c'bd'$. As above, a and b determine a line consisting of the two arcs $[c'd']$. Now $ad' = \frac{1}{2}$ since $ac' = \frac{1}{2}$, $c'd' = 1$, and $c'ad'$. Likewise $bd' = \frac{1}{2}$. Hence

$$ad' + d'b = 1 = ab,$$

so that $d' = \text{mid}(a,b)$. By Theorem 9, $[ad'] + [d'b]$ is a geodesic arc between a and b, obviously not the geodesic arc between a and b which contains c'. Hence the line under discussion consists of the two arcs $[ab]$. If now we let c'' be the second midpoint of a,b and d'' the point such that $c''d'' = 1$, $c''ad''$, and $c''bd''$, then a and b will determine a line formed by the two arcs $[c''d'']$. But, as above, this line also consists of the two arcs $[ab]$, and it is clear that $c'' = d'$ and $c' = d''$. Hence a and b determine a unique line, which is again a simple closed curve of length 2.

13. *Every straight line is congruent to a Euclidean circle of length* 2.

Proof. Let $ab = 1$. Then, as shown in the proof of Theorem 12, *-ab-* consists of the two arcs $[cd]$, where $c = \text{mid}(a,b)$ and d is the unique point such that $cd = 1$, cad, and cbd. We take a Euclidean circle K of length 2, map a,b on any two antipodal points A,B of K, and c,d on C,D, the midpoints of A,B, then map geodesic arcs $[cad]$, $[cbd]$ congruently on semicircles CAD, CBD, respectively. Now if p,q be any distinct points of *-ab-*, and P,Q their corresponding points of K, we must show that $pq = PQ$, where PQ denotes the length of the shorter of the two arcs into which P and Q divide K. Since a,b,c,d divide *-ab-* into four equal quadrants, with a,b the midpoints of c,d, and vice versa, it is easy to see that $pq = PQ$ if p and q are in the same quadrant or in adjacent quadrants. But suppose p,q are interior points of opposite quadrants, e.g., let apc and bqd. Then

$$(pc + cb + bq) + (pa + ad + dq) = 2,$$

so that at least one expression in parentheses, say the first, does not exceed 1. Then $pc + cb + bq \leqslant 1$. Also pcb and cbq. Hence pcq by Axiom 3b, so that $pc + cq = pq \leqslant 1$. Since $PC = pc$, $CQ = cq$ we see that $PC + CQ \leqslant 1$. Hence $PQ = PC + CQ = pq$.

Now let $ab < 1$. Again *-ab-* consists of the two arcs $[cd]$, as above, and we map geodesic arcs $[cad]$, $[cbd]$ congruently on semicircles CAD, CBD, respectively. Let e,f be the midpoints of c,d, chosen so that eac and fbc. Thus we have eac, acb, and $ea + ac + cb < 1$, from which we infer eab by Axiom 3b. Then eac, eab, acb permit us to infer ecb by Theorem 10. Now ecb, cbf, and $ec + cb + bf = 1$ imply ecf by Axiom 3b, and from this we infer ebf by Theorem 10. Hence $ef = ec + cf = 1$, and we infer by Theorem 3 that ecf is a geodesic arc between e and f. Also, since $ed + df = 1 = ef$ we infer that (edf) is a geodesic

arc between e and f. Thus c and d are the midpoints of e and f, as well as vice versa, so that the proof of the congruence of $-ab-$ and K is just like that in the case $ab = 1$ except that now we use e and f instead of a and b.

14. *If $-ab-$ is any straight line and p,q are any distinct points of $-ab-$, then each arc $[pq]$ is contained in $-ab-$.*

Proof. It follows from previous discussions that each arc on $-ab-$ of length $\leqslant 1$ is a geodesic arc. There are two arcs (pq) on $-ab-$. If they are of equal length, each has length 1 and hence is a geodesic arc; in this case $pq = 1$ and $-ab-$ consists of the two arcs $[pq]$. If the two arcs (pq) are unequal in length, only the shorter is a geodesic arc since its length is less than 1; in this case $pq < 1$, there is just one arc $[pq]$, and $-ab-$ contains it.

15. *If $-ab-$ is any straight line and p,q are any distinct points of $-ab-$, then $-pq- = -ab-$.*

Proof. Let $pq = 1$. Then, as shown in the proof of Theorem 12, $-pq-$ consists of the two arcs $[pq]$. In the proof of Theorem 14 we saw that $-ab-$ also consists of these two arcs. Hence $-ab- = -pq-$. Now let $pq < 1$. Then $[pq] \subset -ab-$ by Theorem 14, so that also $r \subset -ab-$, where $r = \text{mid}(p,q)$. Let d be the unique point such that $rd = 1$, rpd, and rqd. Then, as shown in the proof of Theorem 12, $-pq-$ consists of the two arcs $[rd]$. Now let s be the point of $-ab-$ antipodal to r. Then $rs = 1$, rps, and rqs. It follows from Theorem 11 that $d = s$. Hence $-pq-$ consists of the two arcs $[rs]$. But, by the proof of Theorem 14, $-ab-$ also consists of these two arcs. Hence $-ab- = -pq-$.

Combining Theorems 12 and 15 we get:

16. *Any two distinct points are on a unique straight line.*

III. Our space Σ and the S. L. spaces of Busemann

An S. L. space (straight line space) is defined as one satisfying the following five axioms [2]:

A. It is metric.

B. It is finitely compact.

C. It is convex.

D. Each point p has an N-neighborhood $xp < \rho$, $\rho < 0$, such that for any distinct points a,b of N and each $\epsilon > 0$ there is a positive $\delta(a,b,\epsilon) \leqslant \epsilon$ for which a unique point b_σ exists such that $bb_\sigma = \sigma$ and abb_σ.

E. Any two distinct points are on, at most, one geodesic (a geodesic is a locally congruent map of the real axis, and hence is not a geodesic arc).

Clearly Σ has properties A, B, C. To show it has property D, let p be any point and let $\rho < \frac{1}{2}$. If a,b are distinct points in this ρ-neighborhood of p, then $ab \leqslant ap + pb < 1$. Let a,c divide $-ab-$ into equal geodesic arcs. Then b divides one of these arcs into arcs $[ab]$ and $[bc]$, and also abc. Let x be a point such that

abx. Then *abc* and *abx*, so that $c = x$; or *acx*, *bcx*; or *axc*, *bxc* by Theorem 10. Since $ac = 1$, *acx* is impossible, so that x is on the unique arc [*bc*] by Theorem 9. For every positive δ less than *bc* and ϵ there is, of course, a unique point x on [*bc*] such that $bx = \delta$. Thus Σ has property D. To show that Σ has property E we first note that any line *-ab-* is a geodesic since each point of *-ab-* has a neighborhood on *-ab-* which is a geodesic arc. Conversely, if G is any geodesic in Σ it contains two distinct points a,b such that an arc [*ab*] is contained in G. Now a,b determine *-ab-*, which also contains this arc [*ab*]. Thus *-ab-*, a geodesic, and G, also a geodesic, both contain [*ab*]. But in a space with properties A, B, C, D a unique geodesic contains a given geodesic arc [2, p. 21]. Hence G = *-ab-*. It then follows by Theorem 16 that Σ has property E. We have thus proved:

17. *Σ is an* S. L. *space, its straight lines and geodesics being identical.*

Wishing to confine ourselves to plane geometry we assume:

AXIOM 5. Σ is two-dimensional in the sense of Menger-Urysohn.

Since Σ is a two-dimensional S. L. space whose geodesics are all simple closed curves, we can infer the following [2, pp. 79, 81]:

18. *Σ is a projective plane and each two of its straight lines meet in a unique point.*

19. *If p and L are any point and line of Σ, respectively, where $p \not\subset L$, and S is the set of all points on the lines joining p to each point of L, then $S = \Sigma$.*

IV. MOTIONS AND TRANSLATIONS

DEFINITION 2. A *motion* M is a single-valued, distance-preserving transformation of Σ into itself. $M(\alpha,\beta) = \alpha', \beta'$ means that M sends subsets α,β into subsets α',β', respectively. We say α is *fixed* under M if $\alpha' = \alpha$. A sequence of motions M_n *converges* to a motion M if $M_n(x) \to M(x)$ as $n \to \infty$ for each point x of Σ. (The existence of motions other than the identity is assumed later.)

20. *Motions are topological transformations, the set of all motions forming a group.*

21. *Any infinite sequence of motions has a convergent subsequence.*

Proof. If, for an infinite sequence of motions M_n of a finitely compact metric space, a point b exists for which the set $\{M_n(b)\}$ is bounded, then M_n contains a convergent subsequence [2, p. 177]. Σ is finitely compact and bounded. Hence $\{M_n(b)\}$, b being arbitrary, is bounded. The theorem then follows.

22. *Each motion sends between-points into between-points, midpoints into midpoints, conjugate points into conjugate points, geodesic arcs into geodesic arcs, and straight lines into straight lines.*

To arrive at our definition of a translation let us suppose that a motion M has a fixed line L (the existence of motions with fixed lines is formally assumed later). If $[ab] \subset L$ and $M(a,b) = a',b'$, then $M([ab]) = [a'b'] \subset L$. Since L is congruent to a Euclidean circle and M preserves distance on L, it follows that if the oriented geodesic arcs $[ab]$, $[a'b']$ have the same sense so will each oriented geodesic arc $[xy]$ of L and its transform $[x'y'] = M([xy])$ have the same sense, whereas if $[ab]$, $[a'b']$ have unlike senses so will $[xy]$, $[x'y']$ have unlike senses. Thus M is either *sense-preserving* or *sense-reversing* on L.

DEFINITION 3. A *translation* (of Σ) along a line is a motion of Σ leaving that line fixed and preserving sense on it. (The existence of translations is assumed later.)

23. *The set of all translations along the same line forms a group.*

24. *Each infinite sequence of translations along the same line has a subsequence converging to a translation along that line.*

Proof. If L is the line, each infinite sequence of translations along L has a subsequence T_n converging to a motion T by Theorem 21. For any point p of L let $T(p) = p'$, $T_n(p) = p_n$. Then $p_n \subset L$, and $p_n \to p'$ when $n \to \infty$. Line L being a closed set, $p' \subset L$, that is, $T(L) = L$. If $q \subset L$, where $0 < pq < 1$, let $T(q) = q'$, $T_n(q) = q_n$. Then $q_n \to q'$. Since $[pq]$, $[p_nq_n]$ have the same sense, $[p'q']$ has this same sense. T must then preserve sense for all geodesic arcs of L, and hence be a translation along L.

25. *A translation along a line leaving a point of that line fixed leaves each point of the line fixed.*

26. *A translation leaving fixed each of two non-conjugate points leaves fixed each point of their line.*

DEFINITION 4. Distinct translations S, T along the same line are called *equivalent* along the line if $S(x) = T(x)$ for each point x of the line.

27. *Distinct translations S, T along the same line are equivalent along the line if a point p exists on the line so that $S(p) = T(p)$.*

Proof. Let L be the line, x any point of it, $S(p,x) = q,x'$, and $T(x) = x''$. Then $TS^{-1}(q,x') = q,x''$, the translation T being applied second. TS^{-1} leaves each point of L fixed by Theorems 23, 25. Hence $x' = x''$.

28. *Every motion (and hence every translation) has at least one fixed point.*

Proof. A motion being a continuous mapping and Σ being a projective plane, the assertion follows from the fact that a continuous mapping of a projective plane into itself has a fixed point [3, p. 80].

29. *A translation along a line having no fixed point on that line has one fixed point all told.*

Proof. Let T and L be the translation and line, respectively. A point a exists so that $T(a) = a$. Let $b \neq a$, $T(b) = b$. Then $T(\text{-}ab\text{-}, L) = \text{-}ab\text{-}, L$ by Theorem 22. Let $\text{-}ab\text{-}, L$ meet in c. Then $T(c) = c$, which contradicts the hypothesis.

AXIOM 6. Distinct lines G, H exist, each with the property that if a, b are any points on it (not necessarily distinct), there are exactly two distinct translations along it sending a into b.

30. *There is just one translation along G other than the identity leaving each point of G fixed.*

This translation is denoted by R, the identity by I. (A corresponding assertion, of course, holds for H. For brevity we shall usually state things only in terms of G.)

31. *If S, T are equivalent translations along G, then $S^2 = T^2$ and $ST = TS$. Furthermore, $TS^{-1} = S^{-1}T = R$.*

Proof. Let $S(p) = T(p) = q$, where $p \subset G$. Then $T^{-1}S(p) = p$. Hence $T^{-1}S$, a translation along G, leaves each point of G fixed. Suppose $T^{-1}S = I$. Then

$$T(T^{-1}S) = TI = T,$$

so that $(TT^{-1})S = T$, or $IS = T$, and finally $S = T$, which is a contradiction. Hence $T^{-1}S = R$. Likewise

$$TS^{-1} = S^{-1}T = ST^{-1} = R.$$

From $ST^{-1} = S^{-1}T$ and $ST^{-1} = T^{-1}S$, respectively, we get $S^2 = T^2$ and $ST = TS$.

32. *If S, T are equivalent translations along G with no fixed point on G, they have a common fixed point, but no other fixed point.*

Proof. S and T have unique fixed points by Theorem 29, which we denote by f and g, respectively. Suppose $f \neq g$. Let $S(g) = g'$, $T(f) = f'$. Then $g \neq g'$, $f \neq f'$. Also

$$S^2(f) = T^2(f),$$

or $T(f') = f$. Likewise $S(g') = g$. By Theorem 31, $ST(f) = TS(f)$, or $S(f') = f'$, which contradicts the fact that S has f as its only fixed point. Hence $f = g$.

33. *All translations along G have a common fixed point, to be denoted by g.*

Proof. Let a, a_1 be points of G with $aa_1 = \frac{1}{2}$, and T_1 a translation along G such that $T_1(a,g) = a_1,g$, where g is the fixed point of T_1. Let $a_2 = \text{mid}(a,a_1)$ and $T_2(a) = a_2$; $a_3 = \text{mid}(a,a_2)$ and $T_3(a) = a_3$; and in general $a_n = \text{mid}(a,a_{n-1})$ and $T_n(a) = a_n$, where $n > 1$. Then $T_n(g) = g$ for all positive integers n. For any point x, where axa_1, we can construct a translation S from the translations T_n and their limiting translations such that $S(a,g) = x,g$. The powers of all

such translations S send a into all the points of G. Now the totality of translations sending a into all the points of G is identical with the set of all translations along G. Hence if y, z are any points of G, at least one of the two translations along G sending y into z leaves g fixed. Call this translation U, and let V be the equivalent translation along G. If $y \neq z$ then, by Theorem 25, U and V have no fixed point on G; from Theorem 32 and the fact that $U(g) = g$ we then infer that $V(g) = g$. If $y = z$ we note that R and I are the only translations along G sending y into z, and that $I(g) = g$. To show that $R(g) = g$ let T_0, T_+ be any pair of translations equivalent along G, but with no fixed point on G. Then $T_+^{-1}T_0 = R$ by Theorem 31, and $T_0(g) = T_+(g) = g$, as just shown above. From this we see that $R(g) = g$.

34. *Each point of G is conjugate to g.*

Proof. gx is constant for any point x on G by Theorem 33 and Axiom 6. Assume $gx < 1$. Now $R(x,g) = x,g$. It follows from Theorem 26 that R leaves fixed each point of $-gx-$, and hence, by Theorem 19, each point of Σ, so that $R = I$. From this contradiction we infer $gx = 1$.

35. *The translation R has no fixed points other than g and each point of G.*

We let h denote the common fixed point for all translations along H.

36. *The points g and h are distinct, and g is on H if, and only if, h is on G.*

V. Rotations, poles and polars, and reflections

Definition 5. A motion leaving a point c fixed is called a *rotation about c*. If for all points x, y such that $xc = yc$ a rotation about c exists sending x into y, we say that *all rotations about c exist.*

37. *All rotations about g and h exist.*

Proof. Considering only g, let a, b be any points such that $ga = gb$. If a is on G, so is b, in which case a translation along G, that is, a rotation about g, exists sending a into b. Suppose a and b are not on G. Let $-ga- \neq -gb-$, let $-ga-$, $-gb-$ meet G in a', b', respectively, and let S, T be the distinct translations along G such that $S(a') = T(a') = b'$. Now each of these translations sends a into a point of $-gb'-$ whose distance from g equals gb. Let b, b'' be the two points of $-gb'-$ at distance gb from g. S and T cannot both send a into b'', for suppose $S(a) = T(a) = b''$. Since $S(a') = T(a') = b'$, we have $ST^{-1}(b', b'') = b', b''$. Hence ST^{-1}, a translation along G, has b', b'', as well as g, as fixed points. By Theorem 25, then, each point of G is fixed under ST^{-1}, and from Theorem 35 we see that $ST^{-1} = I$, and hence that $S = T$. Since this contradicts the fact that $S \neq T$, we infer that S, T cannot both send a into b''. Similarly they cannot both send a into b. Hence either $S(a) = b$ or $T(a) = b$. Finally, let $-ga- = -gb-$. Then $R(a) = b$, for R leaves $-ga-$ fixed, but not point a, by Theorem 35.

38. *If all rotations about a point p exist, and a motion exists sending p into a point $q(\neq p)$, then all rotations about q exist.*

Proof. Let c, d be any points such that $qc = qd$, and M a motion such that $M(p) = q$, $M^{-1}(c,d) = a,b$. Then $pa = pb$. If N be a rotation about p such that $N(a) = b$, then $MNM^{-1}(q,c) = q,d$.

39. *All rotations exist about some point of G.*

Proof. If $g \subset H$ the assertion is a consequence of Theorems 36 and 37. If $g \not\subset H$, take point $c(\neq g)$ on $-gh-$ so that $hc = hg$. A rotation exists about h sending g into c; hence all rotations about c exist. Take $d(\neq h)$ on $-gh-$, so that $cd = ch$. There is a rotation about c sending h into d; hence all rotations about d exist. Thus we obtain a sequence of points $c,d,e, \ldots$ on $-gh-$ about each of which all rotations exist. The function hx, where x ranges over G, attains its maximum and minimum at points of G since G is a closed set and Σ is compact. Let G and H meet at p; then hp is such a maximum, with the value 1. Let a be a point of G such that ha is a minimum of hx.

Case 1. $gh > ha$. Then $hp > gh > ha$ since $1 > gh$. Since G is connected and closed, hx takes on all values between its maximum hp and minimum ha. Hence for some point $x = x'$ we have $hx' = gh$. A rotation about h exists sending g into x', so that all rotations exist about x', a point of G.

Case 2. $gh < ha$. Let $-gh-$ meet G in r, whence $gh + hr = gr$. Then $ha \leqslant hr$, so that $gh < hr$. The latter relation may be written

$$hr = K \cdot gh + F \cdot gh, \tag{1}$$

where K is a positive integer and $0 \leqslant F < 1$. We then have

$$hr = K \cdot gh + gh - (1 - F)gh,$$

or

$$hr + (1 - F)gh = (K + 1)gh. \tag{2}$$

Since $1 - F > 0$ we infer from (2) that

$$hr < (K + 1)gh. \tag{3}$$

Add gh to each side of (1), obtaining

$$hr + gh = (K + 1)gh + F \cdot gh$$

or

$$gr = (K + 1)gh + F \cdot gh.$$

Since $F \cdot gh \geqslant 0$, we get

$$(K + 1)gh \leqslant gr. \tag{4}$$

From (3) and (4) we have

$$hr < (K + 1)gh \leqslant gr.$$

Since $ha \leqslant hr$ we get

$$ha < (K + 1)gh \leqslant gr.$$

Taking $N = K + 1$, and noting that $gr = hp = 1$, we obtain

$$ha < N \cdot gh < hp.$$

Now we take that one of the points $c,d,e, \ldots$ mentioned previously whose distance from h equals $N \cdot gh$, and denote the point by y. As shown in Case 1 there exists a point on G, which we denote by z, such that $hy = hz$. Hence a rotation about h exists which sends y into z. Since all rotations exist about y they likewise exist about z.

40. *All rotations exist about each point of G and H.*

DEFINITION 6. The locus of points conjugate to any point p is called the *polar* of p, and p is called the *pole* of the locus.

41. *G and H are the polars of g and h, respectively.*

42. *If a motion sends a point p into a point q, it sends the polar of p into the polar of q.*

43. *The polar of each point of G or H is a straight line.*

Proof. Let x be any point of G, and r its conjugate on G. Since $xg = xr = 1$, a rotation exists about x sending g into r. Some translation along G sends r into x. Hence a motion exists sending g into x, and hence G into X, the polar of x. Then X is a straight line by Theorem 22.

DEFINITION 7. A group of motions of a metric space into itself is *transitive* if for each pair of points a,b of the space there exists a motion of the group sending a into b.

44. *The group of all motions of Σ is transitive.*

Proof. Let x,y be any distinct points, p any point of G, P the polar of p, and q the intersection of G and P. Let $x' \subset P$ so that $xg = x'g$. A rotation exists about g sending x into x' by Theorem 37. Since $px' = pq = 1$, a rotation exists about p sending x' into q by Theorem 40. Let $y' \subset G$ so that $py = py'$. Some translation along G sends q into y', and a rotation exists about p sending y' into y. The resultant of these four motions is a motion sending x into y.

45. *All rotations exist about each point of Σ.*

Proof. This follows directly from Theorems 37, 38, 44.

46. *The polar of each point of Σ is a straight line.*

47. *Distinct points have distinct polars.*

Proof. Let a,b be any distinct points, with polars A,B, respectively. If $b \subset A$, clearly $A \neq B$. If $b \not\subset A$, let $-ab-$ meet A in c. Then $ac = 1$ and abc. Thus $ab + bc = ac$, so that $bc < ac$. Since bc, the distance from b to a point of A, is not 1 we infer that $A \neq B$.

48. *Each straight line of* Σ *is the polar of some point.*

Proof. Let C be any line, a,b distinct points of C, and A,B the polars of a,b, respectively. A,B meet in a point c. Then $ca = cb = 1$ since c is on A and B. Hence the polar of c must contain a and b, and must therefore be $\text{-}ab\text{-}$. Thus C is the polar of c.

DEFINITION 8. A *k-dimensional linear subspace* of an S. L. space is any closed k-dimensional set (of the space) which, if it contains any two distinct points, also contains the geodesic through them. An *involutory motion* is a motion, not the identity, whose square is the identity. An involutory motion M of an S. L. space is called a *reflection* in the linear subspace S when all points of S are fixed under M, and S is maximal, i.e., it is not a proper subset of any other linear subspace whose points are fixed under M [2, pp. 113, 179].

49. *Each straight line is a* 1*-dimensional linear subspace of* Σ.

50. *If* p *is any point, and* P *its polar, one of the rotations about* p *is a reflection in* P.

Proof. Let $p = g$. Then $R^2 = I^2$ by Theorem 31, or $R^2 = I$. By Theorem 35 only g, apart from each point of G, is fixed under R. Thus R is a reflection in G by Theorem 49. Now let $p \neq g$, and $M(p) = g$, M being a motion. Then $M(P) = G$. Let x be any point of P, y any point between x and p, and $z(\neq y)$ the point on $\text{-}xp\text{-}$ such that $py = pz$. Let

$$M(x,y,z) = x',y',z',$$

in which case $M(\text{-}xp\text{-}) = \text{-}x'g\text{-}$ and y',z' are on $\text{-}x'g\text{-}$, with $gy' = gz'$. Then

$$M^{-1}RM(p,x) = p,x.$$

Thus the motion $M^{-1}RM$ leaves p, and also each point of P, fixed. But it leaves no other point of Σ fixed. For, suppose $M^{-1}RM(y) = y$, where y is any point of Σ not on P and distinct from p; then $RM(y) = M(y)$, or $R(y') = y'$, where, as above, $M(y) = y'$. But this contradicts Theorem 35. Now $M^{-1}RM \neq I$, otherwise $R = I$. Also $R(y') = z'$ since $gy' = gz'$. Hence

$$M^{-1}RM(p,x,y,z) = p,x,z,y,$$

so that $(M^{-1}RM)^2 = I$. Also $M^{-1}RM$ leaves fixed each point of the linear subspace P, and P is maximal. Hence $M^{-1}RM$ is a reflection in P, and since it leaves p fixed it is also a rotation about p.

From Theorems 48 and 50 we then obtain:

51. *A reflection exists in each straight line of* Σ.

DEFINITION 9. A metric space is called *homogeneous* if and only if it is congruent to a Euclidean, hyperbolic, or elliptic space of finite dimension.

52. Σ *is congruent to a two-dimensional elliptic space.*

Proof. An S. L. space is homogeneous if a reflection exists in each geodesic [2, p. 181]. Hence Σ is homogeneous by Theorems 17 and 51 and, being a projective plane, must be congruent to a two-dimensional elliptic space.

VI. A final remark on Σ and S. L. spaces

Busemann states that if all translations exist along two geodesics of a closed S. L. plane, the metric of the latter is elliptic [2, p. 219]. The proof of this, which was left to the writer, can now be supplied. For brevity we merely outline its main features. First, we can use results in [2] to show that Axioms 1 to 5 for Σ are valid propositions in any closed S. L. plane S. Thus S is a compact metric space, two points at maximum distance have exactly two midpoints, etc. Then, noting that Busemann's translations are defined somewhat differently than are translations in Σ, we can show, nevertheless, that the assumption that all of Busemann's translations exist along a geodesic of S implies that exactly two translations as defined in Σ exist along it, sending an arbitrary one of its points into an arbitrary one of its points. Then, whenever all Busemann's translations exist along two geodesics of S, so do all translations exist along them in the sense of Axiom 6. It follows that Axioms 1 to 6 are valid propositions in S if all Busemann's translations exist along two geodesics of S. The metric of S would then be elliptic by Theorem 52.

References

1. L. M. Blumenthal, *Metric characterization of elliptic space*, Trans. Amer. Math. Soc., vol. 59 (1946), 381-400.
2. Herbert Busemann, *Metric methods in Finsler spaces and in the foundations of geometry* (Ann. Math. Studies, No. 8, Princeton, 1942).
3. W. Fenchel, *Elementare Beweise und Anwendungen einiger Fixpunktsätze*, Mat. Tids., B (1932), 66-87.
4. K. Menger, *Untersuchungen über allgemeine Metrik*, Math. Ann., vol. 100 (1928), 74-113.

New York University

ON THE GEOMETRY OF LINEAL ELEMENTS ON A SPHERE, EUCLIDEAN KINEMATICS, AND ELLIPTIC GEOMETRY

J. M. FELD

1. Introduction. The geometry of *slides* and *turns* of oriented lineal elements in the plane was first studied by Kasner [10]. Slides and turns generate *whirls*, which constitute a three-parameter group W_3. The product of W_3 and M_2, the three-parameter group of Euclidean displacements in the plane, yields a six-parameter group of *whirl-motions*[1] G_6. The geometry of *turbines*[2], and also of general series of lineal elements, under G_6 was investigated by Kasner in [10] and, in subsequent papers, by Kasner and DeCicco, particularly in [3], [4], [11], [12]. The author investigated the geometry of series of lineal elements under the seven-parameter group of *whirl-similitudes* G_7 (of which G_6 is a subgroup) in [6], [7], [8]. Among other things, the author showed that G_7 is isomorphic to the group of collineations of the points in *quasi-elliptic* three-space, the geometry of which had been previously studied by Blaschke [1], [2] and Grünwald [9]; he also showed how the geometry of W_3, G_6, and G_7 can be interpreted kinematically as the displacement of one plane over another.

In this paper we investigate the geometry of *spherical whirls* and *whirl-rotations* of oriented lineal elements on a sphere. Some results in this field have already been obtained by Strubecker [15], who mapped the points of elliptic three-space E_3 one-to-one upon the oriented lineal elements of a unit sphere. Using synthetic methods, Strubecker deduced, from the geometry of lines in E_3, theorems on *spherical turbines* and families of curves on a sphere, analogous to others found by Kasner for the plane [10]. We pursue the geometry of whirls and whirl-rotations on a sphere in other directions and by means of other methods. With the aid of quaternions we shall investigate the differential geometry of series of lineal elements on a sphere subject to two groups, $\mathfrak{W}_3$ and $\mathfrak{G}_6$—analogous respectively to W_3 and G_6 in the plane—determining their fundamental differential invariants and "Serret-Frenet formulae." Our principal objective is to present a characterization of the geometry of whirls and whirl-rotations on a sphere in terms of the kinematic geometry of continuous

Received October 16, 1950; presented to the American Mathematical Society February 25, 1950.

[1]Slides and turns of *non-oriented* lineal elements in the plane had been previously used by Scheffers [14] in an investigation of certain groups of contact transformations. Whirls are not contact transformations.

[2]A *turbine* is a series of oriented lineal elements the points of which lie on a circle (which may be a point circle), and the (oriented) lines of which are tangent to a concentric oriented circle.

Turbines in space were studied by A. Narasinga Rao [13] and Feld [5].

displacements of one unit sphere over another, similar to the kinematic interpretation we gave in [8] of whirls and whirl-motions in the plane in terms of continuous displacements of one plane over another. The use of quaternions has the advantage of making it particularly easy to map oriented lineal elements on a sphere into the points of E_3. We indicate by means of this mapping how the differential geometry under $\mathfrak{G}_6$ of series on a sphere can serve as a model for the geometry of curves in E_3.

2. Whirl-rotations and turbines. Let the unit sphere S have its centre at the origin O of a right-hand orthogonal coordinate frame $\mathfrak{f}_0$. If an oriented lineal element $\mathfrak{e}$ is tangent to S at the point P, we shall call the great circle through P tangent to $\mathfrak{e}$ and oriented like $\mathfrak{e}$ the *great cycle* of $\mathfrak{e}$. Let the lineal element $\mathfrak{e}_0$ have its point at (1,0,0) and let it be directed so that its great cycle passes through (0,1,0) and is oriented in the counter-clockwise sense, when viewed from the point (0,0,1). We shall call $\mathfrak{e}_0$ the primitive lineal element on S, and $\mathfrak{f}_0$ its *associated frame.*

Let e_0, e_1, e_2, e_3 be the quaternion units such that

$$e_0e_i = e_ie_0 = e_i; \qquad e_1^2 = e_2^2 = e_3^2 = e_1e_2e_3 = -1;$$

and let

$$x = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3, \qquad \bar{x} = x_0e_0 - x_1e_1 - x_2e_2 - x_3e_3.$$

Then a rotation of S around an oriented diameter is given by Hamilton's formula

$$N(x)u^* = \bar{x}ux, \qquad N(x) = x\bar{x},$$

where u and u^* are unit vectors emanating from O. The components x_i of x are the homogeneous Euler parameters of the rotation. If $\mathfrak{e}$ is any lineal element on S and x is the quaternion of the rotation $\mathfrak{e}_0 \to \mathfrak{e}$, we shall call the components of x the homogeneous coordinates of $\mathfrak{e}$. For convenience, when no confusion will result, we shall let the quaternion x designate both the rotation $\mathfrak{e}_0 \to \mathfrak{e}$ and the lineal element $\mathfrak{e}$. Evidently, if x designates $\mathfrak{e}$, so does kx, where k is a non-zero scalar. If $N(x) = 1$, we shall call x a normalized quaternion and represent it in bold type: $\mathbf{x}$. To any quaternion x, $N(x) \neq 0$, correspond two normalized ones, namely $\pm x/[N(x)]^{\frac{1}{2}}$. If the rotation x rotates $\mathfrak{e}_0 \to \mathfrak{e}$ around the unit vector v through the angle 2θ, we can let

$$\mathbf{x} = -\cos\theta + v\sin\theta$$

and

$$-\mathbf{x} = -\cos(\pi - \theta) + \bar{v}\sin(\pi - \theta) \qquad (\bar{v} = -v).$$

The rotation x also rotates $\mathfrak{f}_0$ into another Cartesian frame $\mathfrak{f}$, situated relative to $\mathfrak{e}$ as $\mathfrak{f}_0$ is situated relative to $\mathfrak{e}_0$; we shall call $\mathfrak{f}$ the frame associated with $\mathfrak{e}$.

A lineal element transformation $x \to x^*$ given by the equation (in which we suppress the factor of proportionality)

$$x^* = xa, \tag{2.1}$$

where

$$\mathbf{a} = -\cos\alpha + u\sin\alpha \qquad (u^2 = -1),$$

represents a rotation of all the lineal elements on S around the unit vector u through the angle 2α. We shall call such transformations *lineal element rotations*, and we shall let the quaternion a represent the lineal element rotation (2.1). The lineal element rotations constitute a three-parameter group $\mathfrak{M}_3$.

A lineal element transformation $x \to x^*$ whereby every lineal element x is rotated through the same angle 2β around a unit vector u_x, situated relative to the frame $\mathfrak{f}$ associated with x as an arbitrarily given unit vector u_0 is situated relative to $\mathfrak{f}_0$, shall be called a *(spherical) whirl*.

Let the rotation around u_0 through the angle 2β be denoted by the quaternion b where

$$\mathbf{b} = -\cos\beta + u_0\sin\beta.$$

Then $x^*\bar{x} = x\bar{x}b$, so that the whirl $x \to x^*$ is given within a factor of proportionality by the equation

$$x^* = bx. \tag{2.2}$$

The whirls constitute a three-parameter group of lineal element transformations $\mathfrak{W}_3$, skew-isomorphic to $\mathfrak{M}_3$.

The product of a whirl and a lineal element rotation is commutative. A transformation which is the product of a whirl and a lineal element rotation shall be called a *whirl-rotation*. Whirl-rotations $x \to x^*$ are given by the equation (the factor of proportionality being suppressed)

$$x^* = bxa. \tag{2.3}$$

The whirl-rotations constitute a six-parameter group $\mathfrak{G}_6$.

Let the symbol (x,y) represent the *scalar product* of two lineal elements x and y, defined as follows:

$$(x, y) = \tfrac{1}{2}(x\bar{y} + y\bar{x}).$$

Since $x\bar{y} + y\bar{x} = \bar{x}y + \bar{y}x$, we also have

$$(x, y) = \tfrac{1}{2}(\bar{x}y + \bar{y}x).$$

With the aid of this definition we obtain the following useful equalities:

$$\begin{aligned} &(x, y) = (y, x), \qquad (x, x) = N(x) = x\bar{x}, \\ &(ax, y) = (x, ay) = a(x, y) \qquad (a \text{ a scalar}), \\ &(x, y + z) = (x, y) + (x, z), \\ &(bxa, bxy) = (a, a)(b, b)(x, y). \end{aligned} \tag{2.4}$$

Since $N(\mathbf{x}\bar{\mathbf{y}}) = 1$, we can let $\mathbf{x}\bar{\mathbf{y}}$ equal either $-\cos\delta + v\sin\delta$ or $-\cos(\pi - \delta) + \bar{v}\sin(\pi - \delta)$, $v^2 = -1$. Therefore $(\mathbf{x},\mathbf{y}) = -\cos\delta$ in the former case and $-\cos(\pi - \delta)$ in the latter. Thus $\cos\delta = \pm(\mathbf{x},\mathbf{y})$. We shall call δ and $\pi - \delta$ $(0 \leqslant \delta \leqslant \pi)$, the *distances* between x and y: x and y coincide only when $\delta = 0$ or π.

Evidently

$$\cos^2 \delta = \frac{(x, y)^2}{(x, x)(y, y)}. \tag{2.5}$$

If $(x,y) = 0$, in which case $\delta = \frac{1}{2}\pi$, we shall say that x and y are *orthogonal*.

If we subject x and y to the whirl-rotation (2.3) we obtain, by virtue of the last equation in (2.4),

$$(x^*, y^*) = (a, a)\ (b, b)(x, y).$$

This yields

THEOREM 2.1. *Under the group of whirl-rotations a pair of elements x and y have an invariant $\cos^2 \delta$, given by (2.5), δ and $\pi - \delta$ being the distances between x and y.*

Let the lineal elements x and y be distinct, that is, $\cos^2 \delta \neq 1$. The ∞^1 lineal elements z defined by the equation

$$z = \alpha x + \beta y \qquad (\alpha, \beta \text{ real scalars}, \alpha^2 + \beta^2 \neq 0), \tag{2.6}$$

shall be called a *linear series* of lineal elements. From (2.6) we obtain with the aid of (2.4)

$$(x, z) = \alpha(x, x) + \beta(x, y),$$

$$(y, z) = \alpha(x, y) + \beta(y, y),$$

$$(z, z) = \alpha(x, z) + \beta(y, z).$$

Eliminating α and β, we obtain

$$D = \begin{vmatrix} (x, x) & (x, y) & (x, z) \\ (y, x) & (y, y) & (y, z) \\ (z, x) & (z, y) & (z, z) \end{vmatrix} = 0. \tag{2.7}$$

The following theorems can now be easily established.

THEOREM 2.2. *Two distinct lineal elements determine a linear series.*

THEOREM 2.3. *A necessary and sufficient condition that three lineal elements x,y and z lie on a linear series is that $D = 0$.*

Let q, $N(q) = 1$, be a given lineal element, and let $a = -\cos\theta + r \sin\theta$, where r is a constant unit vector and θ is variable. The lineal element

$$x = qa, \quad N(q) = 1, \tag{2.8}$$

is obtained by rotating q around the vector r through the angle 2θ. It will be convenient hereafter to let a unit vector v designate also the point on S that has for its Cartesian coordinates the components of v. As θ varies from 0 to π, x describes a series of lineal elements, the points of which lie on a circle c (which may be a point circle) having its centre at r, and the great cycles of which make

the same angle with c. Such a series shall be called a *spherical turbine;* c shall be called the circle of the turbine, and the points r and $-r$ the centres of the turbine. If we select three lineal elements (2.8) by assigning three arbitrary values to θ, we find that their quaternions satisfy (2.7); consequently, spherical turbines are linear series.

Let us define

$$l = qr\bar{q}.$$

Evidently l is a constant unit vector. Since

$$xr\bar{x} = (qa)r(\overline{qa}) = q(ar\bar{a})\bar{q} = qr\bar{q} = l,$$

the turbine $\mathfrak{T}$ defined parametrically by means of (2.8) has the non-parametric equation

$$\bar{x}lx = r, \qquad (x\bar{x} = 1). \tag{2.9}$$

But the equation of $\mathfrak{T}$ can also take the form $\bar{x}(-l)x = -r$; therefore, the lineal elements of $\mathfrak{T}$ are represented by those quaternions x which correspond to the rotations of the unit sphere S that carry point l to r, and point $-l$ to $-r$; that is to say, the quaternions x correspond to the rotations of S that carry the oriented diameter $-l \to l$ into $-r \to r$.

3. The kinematic representation of turbines. Let us consider two concentric unit spheres S_l (the left sphere) and S_r (the right sphere). Let the pair of diametrically opposite points l and $-l$ lie on S_l, and let the pair of points r and $-r$ lie on S_r. We can now map the turbine $\mathfrak{T}$ upon two ordered pairs of points on S_l and S_r, namely, l,r and the diametrically opposite pair $-l, -r$. We shall call l,r (or, alternatively, $-l, -r$) respectively the *left* and *right coordinates* of $\mathfrak{T}$, and let either of the symbols $[l, r]$ or $[-l, -r]$ represent $\mathfrak{T}$. Let this mapping whereby every turbine $\mathfrak{T}$ on S corresponds to two pairs of image points on S_l and S_r be called the ***kinematic representation*** $\mathscr{K}$. We can make $\mathscr{K}$ one-to-one by orienting the turbines on S. With every turbine $\mathfrak{T}$ we associate two oriented turbines $\mathfrak{T}^+$ and $\mathfrak{T}^-$ by assigning to $\mathfrak{T}^+$ the centre r and to $\mathfrak{T}^-$ the centre $-r$. A one-to-one kinematic representation of *oriented turbines* is brought about by choosing the pair of points l,r as the image and $[l, r]$ as the symbol of $\mathfrak{T}^+$, and the pair $-l, -r$ as the image and $[-l, -r]$ as the symbol of $\mathfrak{T}^-$. The simultaneous reflection of the points on S_l and S_r in their common centre corresponds to a reversal of the orientation of the turbines on S.

Let $\mathfrak{T}$: $[l, r]$ be the turbine determined by the two lineal elements x and y. The parametric equation (2.8) of $\mathfrak{T}$ yields

$$\mathbf{y} = \mathbf{x}(-\cos\theta + r\sin\theta).$$

Since

$$\bar{\mathbf{x}}\mathbf{y} + \bar{\mathbf{y}}\mathbf{x} = -2\cos\theta,$$

θ is a distance between x and y; moreover, since

$$\bar{\mathbf{x}}\mathbf{y} - \bar{\mathbf{y}}\mathbf{x} = 2r \sin\theta = 2r \sin\delta,$$

where δ is either distance between x and y, we obtain

THEOREM 3.1. *The turbine determined by the lineal elements x, y ($\mathbf{x} \neq \pm \mathbf{y}$), has turbine coordinates l, r given by the formulae*

$$l = \frac{y\bar{x} - x\bar{y}}{2\{(x,x)(y,y)\}^{\frac{1}{2}}} \csc\delta, \quad r = \frac{\bar{x}y - \bar{y}x}{2\{(x,x)(y,y)\}^{\frac{1}{2}}} \csc\delta,$$

where δ is a distance between x and y.

Evidently all turbines have the same "length" π.

Because equation (2.9) can be regarded as a necessary and sufficient condition for the incidence of a turbine $[l,r]$ and a lineal element $\mathbf{x}$, we obtain

THEOREM 3.2. *To the ∞^2 oriented turbines $\mathfrak{T}$ incident to a given lineal element x on S correspond, by virtue of the one-to-one mapping $\mathcal{K}$, ∞^2 left image points l on S_l and ∞^2 right image points r on S_r, so that the rotation of S_l that corresponds to the quaternion x brings the ∞^2 left image points into coincidence with their ∞^2 associated right image points.*

The whirl-rotation (2.3) transforms $[l, r]$ into $[l^*, r^*]$ where $l^* = \mathbf{b}\, l\, \bar{\mathbf{b}}$, $r^* = \bar{\mathbf{a}}\, r\, \mathbf{a}$.

The set of ∞^2 lineal elements orthogonal to a given lineal element u shall be called a *planar field* The elements x of this planar field $\mathfrak{F}$ are given by the parametric equation

$$x = ua, \quad a + \bar{a} = 0, \quad a\bar{a} = 1. \tag{3.1}$$

Eliminating a we obtain the non-parametric equation of $\mathfrak{F}$:

$$\bar{u}x + \bar{x}u = 0. \tag{3.2}$$

The four components of u determine $\mathfrak{F}$ and shall be called the homogeneous coordinates of $\mathfrak{F}$.

If the lineal elements y and z lie in the field u, $x = \alpha y + \beta z$ (α and β real scalars) satisfies (3.2) identically. Therefore the turbine determined by y and z lies in u.

By means of the whirl-rotation $x \to bxa$ the planar field u is transformed into the planar field u^* where

$$u^* = bua. \tag{3.3}$$

Hence we obtain

THEOREM 3.3. *Whirl-rotations transform planar fields into planar fields.*

We can regard (3.3) as the equation of $\mathfrak{G}_6$ in planar field coordinates.

If the lineal elements y and z determine the turbine $[l, r]$, then, in order that $[l, r]$ lie in the field u, it is necessary and sufficient that y and z satisfy (3.2). Hence

$$\bar{\mathbf{u}}y = -\bar{y}\mathbf{u}, \qquad \bar{\mathbf{u}}z = -\bar{z}\mathbf{u},$$

and therefore

$$\bar{z}y = \bar{\mathbf{u}}z\bar{y}\mathbf{u}, \quad . \quad \bar{y}z = \bar{\mathbf{u}}y\bar{z}\mathbf{u};$$

consequently

$$\bar{y}z - \bar{z}y = \bar{\mathbf{u}}(y\bar{z} - z\bar{y})\mathbf{u}.$$

Using the formulae for l and r given in Theorem 3.1 we obtain

$$\bar{\mathbf{u}}/\mathbf{u} = -r \tag{3.4}$$

as a necessary and sufficient condition that the turbine $[l, r]$ lie in the field u. We now have

THEOREM 3.4. *By means of $\mathscr{K}$ the ∞^2 oriented turbines that lie in a planar field u are mapped upon pairs of points l, r on S_l and S_r respectively, so that a symmetry (that is, an improper orthogonal transformation) will transform the left image points into their corresponding right image points; the homogeneous Euler parameters of this symmetry are the coordinates of the planar field u.*

The companion Theorems 3.2 and 3.4 justify calling $\mathscr{K}$ a kinematic representation.

Inasmuch as planar fields are transformed like lineal elements by whirl-rotations, we define the angles ϕ and $\pi - \phi$, $0 \leqslant \phi < \pi$, between the two planar fields u and v by an expression dual to that used for the distances between two lineal elements, namely,

$$\cos^2 \phi = \frac{(u, v)^2}{(u, u)(v, v)}. \tag{3.5}$$

Let the lineal element u be called the *pole* of the planar field u. The following theorems are now easily established.

THEOREM 3.5. *The angle between two planar fields is equal to the distance between their poles.*

THEOREM 3.6. *Two planar fields u and v intersect in a turbine $[l,r]$ where*

$$l = \frac{(u\bar{v} - v\bar{u}) \csc \phi}{2\{(u, u)(v, v)\}^{\frac{1}{2}}}, \qquad r = \frac{(\bar{u}v - \bar{v}u) \csc \phi}{2\{(u, u)(v, v)\}^{\frac{1}{2}}}$$

and ϕ is either one of the angles between u and v.

If x, y and z are three linearly independent lineal elements, there exists a unique lineal element u orthogonal to all of them. Since u must satisfy the equations

$$\bar{u}x + \bar{x}u = \bar{u}y + \bar{y}u = \bar{u}z + \bar{z}u = 0,$$

the components of u are given by

$$u_0 : u_1 : u_2 : u_3 = |x_1 y_2 z_3| : -|x_0 y_2 z_3| : |x_0 y_1 z_3| : -|x_0 y_1 z_2|.$$

This yields

THEOREM 3.7. *A planar field is determined by three linearly independent lineal elements.*

THEOREM 3.8. *If x, y, and z are linearly independent lineal elements, the ∞^2 lineal elements*

$$w = \alpha x + \beta y + \gamma z \qquad (\alpha, \beta, \gamma \text{ real numbers})$$

constitute the planar field determined by x, y, and z.

4. Differential invariants of series of lineal elements under $\mathfrak{W}_3$ and $\mathfrak{M}_3$. A series of lineal elements on S is a one-dimensional extent of lineal elements defined by

$$x = x(t) \tag{4.1}$$

where t is a real parameter. We assume that $dx/dt \neq 0$ in the interval $t_1 \leqslant t \leqslant t_2$ and that $x(t)$ has a continuous second derivative. We can, without loss of generality, also assume that $x(t)$ is normalized, that is, that

$$x(t)\bar{x}(t) = 1. \tag{4.2}$$

In addition we assume, as we may, that the quaternions a and b that appear in the lineal element rotation $x \to xa$ and whirl $x \to bx$ are normalized, so that normalized series are transformed by these transformations into normalized series.

Let the whirl b transform the series $\mathfrak{S}$: (4.1) into the series $\mathfrak{S}^*$: $x^*(t)$. Then

$$d\sigma^2 = d\bar{x}dx = d\bar{x}^*dx^*$$

is invariant. We shall call

$$\sigma = \int_{t_0}^{t} \left(\frac{dx}{dt}\frac{d\bar{x}}{dt}\right)^{\frac{1}{2}} dt$$

the $\mathfrak{W}_3$-arc length of $\mathfrak{S}$ measured from t_0 to t. Let the equation of $\mathfrak{S}$ be expressed in terms of the invariant parameter σ. Then, letting $x' = dx/d\sigma$, we have

$$\bar{x}(\sigma)x(\sigma) = 1, \quad \bar{x}'x' = 1. \tag{4.3}$$

Evidently

$$Z = \bar{x}x' \tag{4.4}$$

is a differential invariant under $\mathfrak{W}_3$. Equations (4.3) yield

$$\bar{x}x' + \bar{x}'x = 0, \qquad N(x) = N(x') = 1. \tag{4.5}$$

Therefore $Z(\sigma)$ is a unit vector. The three components of Z, namely Z_i (i = 1,2,3) where $\sum Z_i^2 = 1$, are differential scalar invariants of $\mathfrak{S}$ under $\mathfrak{W}_3$.

We proceed to find geometric interpretations for σ and Z. Let us consider the distance $\Delta\delta$ between the lineal elements $x(\sigma)$ and $x(\sigma + \Delta\sigma)$ on $\mathfrak{S}$. Since

$$2\cos\Delta\delta = \bar{x}(\sigma)x(\sigma + \Delta\sigma) + \bar{x}(\sigma + \Delta\sigma)x(\sigma)$$

(see §3), we obtain

$$2\left(\frac{d\delta}{d\sigma}\right)^2 = -(\bar{x}x'' + \bar{x}''x).$$

But differentiation of the first equation in (4.5) yields

$$\bar{x}x'' + \bar{x}''x = -2. \tag{4.6}$$

Hence

$$d\sigma = \pm d\delta.$$

Next, let us consider the turbine $\mathfrak{T}:[l,r]$ with centres at r and $-r$, tangent to $\mathfrak{S}$ at σ_0. By Theorem 3.1

$$r = \lim_{\Delta\sigma\to 0} \tfrac{1}{2}[\bar{x}(\sigma_0)x(\sigma_0+\Delta\sigma) - \bar{x}(\sigma_0+\Delta\sigma)x(\sigma_0)] \csc \Delta\sigma.$$

Since $\bar{x}x'$ is a unit vector, we obtain

$$r = \tfrac{1}{2}[\bar{x}(\sigma_0)x'(\sigma_0) - \bar{x}'(\sigma_0)x(\sigma_0)] = \bar{x}(\sigma_0)x'(\sigma_0) = Z(\sigma_0).$$

Therefore $Z(\sigma)$ and $-Z(\sigma)$ are the loci of the centres of the turbines tangent to the series $\mathfrak{S}$.

Under the group $\mathfrak{M}_2$ we obtain the same invariant parameter σ as under $\mathfrak{W}_2$, and we assume again that $\mathfrak{S}$ is expressed in terms of this parameter. It is evident that the unit vector

$$W = x'\bar{x} \tag{4.7}$$

is invariant under $\mathfrak{M}_2$. The turbine tangent to $\mathfrak{S}$ at σ_0 has a left image vector l which, by Theorem 3.1, is given by

$$\begin{aligned} l &= \lim \tfrac{1}{2}[x(\sigma_0+\Delta\sigma)\bar{x}(\sigma_0) - x(\sigma_0)\bar{x}(\sigma_0+\Delta\sigma)] \csc \Delta\sigma \\ &= x'(\sigma_0)\bar{x}(\sigma_0) = W(\sigma_0). \end{aligned}$$

Consequently we obtain a geometric interpretation of the differential invariant $W(\sigma)$ of $\mathfrak{S}$ under $\mathfrak{M}_2$, namely, the locus of the left image point l of the turbines tangent to $\mathfrak{S}$.

Differential invariants of $\mathfrak{S}$ of higher order relative to $\mathfrak{W}_2$ [$\mathfrak{M}_2$] result from differentiating $Z(\sigma)$ [$W(\sigma)$] with respect to σ.

To find kinematic interpretations for $Z(\sigma)$ and $W(\sigma)$, we proceed as follows:

Let S_f and S_m be two unit spheres concentric at O; S_f is fixed in position but S_m is mobile around O. Let $\mathfrak{e}_f$ be a primitive lineal element on S_f and let F_f be its associated rectangular Cartesian frame. Let $\mathfrak{e}_m$ be an arbitrary (primitive) lineal element on S_m and F_m its associated frame; $\mathfrak{e}_m$ and its frame F_m are mobile with S_m relative to S_f and $\mathfrak{e}_f$. Lineal elements and points on S_f will be referred to $\mathfrak{e}_f$ and F_f, but lineal elements and points on S_m will be referred both to $\mathfrak{e}_m$ and $\mathfrak{e}_f$, or, what is equivalent, to their associated frames. Let the initial position of $\mathfrak{e}_m$, and therefore also of S_m, relative to $\mathfrak{e}_f$ be given by the quaternion x_0, namely, the quaternion of the rotation $\mathfrak{e}_f \to \mathfrak{e}_m$. As S_m undergoes a continuous displacement $\mathfrak{D}$ around O, $\mathfrak{e}_m$ traces on S_f a series $\mathfrak{S}$ which, referred to $\mathfrak{e}_f$, has

the equation $x = x(\sigma)$, where $x_0 = x(\sigma_0)$ denotes the initial position of $\mathfrak{e}_m$. $\mathfrak{S}$ defines completely the displacement $\mathfrak{D}$. But $\mathfrak{D}$ can be defined as well by a series $\mathfrak{S}^*$ traced on S_f by any other lineal element $\mathfrak{e}^*_m$ on S_m. Let the quaternion that determines the position of $\mathfrak{e}^*_m$ relative to $\mathfrak{e}_f$ be x^*_0; then, if $x^*_0 = bx_0$ is the whirl $\mathfrak{e}_m \to \mathfrak{e}^*_m$, this whirl also transforms $\mathfrak{S} \to \mathfrak{S}^*$.

Let P be a point on S_m, and let its coordinates, when referred to $\mathfrak{e}_m$, be the components of the unit vector v. Then, referred to $\mathfrak{e}_f$ on S_f, P has for its coordinates the components of the unit vector

$$V = \bar{x}vx, \tag{4.8}$$

because the rotation that transports $\mathfrak{e}_f \to \mathfrak{e}_m$ transforms $v \to V$. During the motion $x(\sigma)$ of S_m the vector V describes a cone, the intersection of which with S_f is the trajectory that the point P of S_m traces on S_f. To find the *poles* (instantaneous centres of rotation) of the motion, we seek those points V on S_f for which $V'(\sigma) = O$. From (4.8) we get $xV' + x'V = vx'$. Consequently $V = \bar{x}'vx'$, and therefore $x'V\bar{x}' = v = xV\bar{x}$. Hence

$$V = \bar{x}'xV\bar{x}x',$$

which implies that V is collinear with the vector $\bar{x}x'$. Therefore the locus of the pole on the fixed sphere (the *fixed* or *space centrode*) is $\pm Z(\sigma)$.

The locus of the pole on the mobile sphere (the *mobile* or *body centrode*), referred to $\mathfrak{e}_m$, is

$$v = xV\bar{x} = x(\pm Z)\bar{x} = \pm x\bar{x}x'\bar{x} = \pm x'\bar{x} = \pm W(\sigma). \tag{4.9}$$

During the displacement $\mathfrak{D}$ defined by the series $\mathfrak{S}$, the curve $W(\sigma)$ on S_m rolls without slipping on the curve $Z(\sigma)$ on S_f, while, of course, $-W(\sigma)$, diametrically opposite to $W(\sigma)$ on S_m, rolls on $-Z(\sigma)$. The motion $\mathfrak{D}$ is completely determined by the centrodes $Z(\sigma)$ and $W(\sigma)$, which, in turn, are determined by $\mathfrak{D}$. However, it should be observed that the equation of the mobile centrode is referred not to $\mathfrak{e}_f$ but to any lineal element of $\mathfrak{S}$, say to $\mathfrak{e}_m : x(\sigma_0)$. Therefore, if we replaced on S_m the primitive element $\mathfrak{e}_m$ by another primitive element $\mathfrak{e}^*_m : x^*$, the motion $\mathfrak{D}$ that was defined by the series $\mathfrak{S}$ traced out on S_f by $\mathfrak{e}_m$ would instead be defined by a series $\mathfrak{S}^*$ traced out on S_f by $\mathfrak{e}^*_m$. But now the mobile centrode would be referred to $\mathfrak{e}^*_m$ and, according to (4.9), would be given by $W = \pm x^*Z\bar{x}^*$. Consequently the motion $\mathfrak{D}$ is determined by the fixed centrode $\pm Z(\sigma)$ and an arbitrary primitive lineal element. If w is the whirl $\mathfrak{e}_m \to \mathfrak{e}^*_m$, w transforms the series $\mathfrak{S}$ generated by $\mathfrak{e}_m$ into the series $\mathfrak{S}^*$ generated by $\mathfrak{e}^*_m$. Since $\mathfrak{S}$ and $\mathfrak{S}^*$ define the same motion $\mathfrak{D}$, and $\mathfrak{D}$ is defined by $\pm Z(\sigma)$ and an arbitrary lineal element on S_m, $Z(\sigma)$ determines a series within a whirl. We can therefore regard $Z = Z(\sigma)$ as the intrinsic equation of a series relative to $\mathfrak{W}_3$.

The motion defined by a turbine $[l, r]$ is a continuous rotation of S_m around the diameter $(-l \to l)$, and therefore has for its fixed [mobile] centrode the pair of diametrically opposite points $\pm r[\pm l]$. If $\mathfrak{D}$ is a displacement defined by

a series $\mathfrak{S}$ other than a turbine, the fixed [mobile] centrode of $\mathfrak{D}$ is the locus of the right [left] image points $\pm r(\sigma)$ [$\pm l(\sigma)$] of the turbines tangent to $\mathfrak{S}$.

5. Differential invariants of series under $\mathfrak{G}_6$. Let the series $\mathfrak{S}$ have the equation

$$x = x(t), \qquad x(t)\bar{x}(t) = 1, \tag{5.1}$$

where $x(t)$ has a continuous third derivative in the interval $t_1 \leqslant t \leqslant t_2$ in which $dx/dt \neq 0$. Subjecting $\mathfrak{S}$ to the whirl-rotation

$$x^* = bxa, \qquad N(a) = N(b) = 1,$$

we obtain

$$dx^* d\bar{x}^* = b\,dx\,a\bar{a}\,d\bar{x}\,\bar{b} = dx\,d\bar{x}.$$

We let the invariant $dx\,d\bar{x} = d\sigma^2$ as before, but now we designate

$$\sigma = \int_{t_0}^{t} \left(\frac{dx}{dt}\frac{d\bar{x}}{dt}\right)^{\frac{1}{2}} dt$$

as the $\mathfrak{G}_6$-arc length of $\mathfrak{S}$ measured from t_0 to t. Let the parameter t in (5.1) be expressed in terms of σ; then the equation of $\mathfrak{S}$ becomes $x = x(\sigma)$ where

$$x(\sigma)\bar{x}(\sigma) = 1, \qquad x'(\sigma)\bar{x}'(\sigma) = 1. \tag{5.2}$$

We shall consider only series $x(\sigma)$ for which

$$(x'', x'') - 1 \neq 0$$

in the interval $\sigma_1 \leqslant \sigma \leqslant \sigma_2$. The significance of this restriction will be explained later.

Let us associate with any lineal element σ of $\mathfrak{S}$ in the interval $(\sigma_1\sigma_2)$ a frame composed of four mutually orthogonal lineal elements represented by the normalized quaternions ξ_i $(i = 1,2,3,4)$ in the following manner:

According to (5.2), x and x' are normalized quaternions. Moreover,

$$x\bar{x}' + x'\bar{x} = 2(x, x') = 0. \tag{5.3}$$

Therefore x and x' are orthogonal lineal elements. Let

$$\xi_1 = x, \quad \xi_3 = x'. \tag{5.4}$$

The second equations in (5.2) and (5.3) yield

$$(x', x'') = 0, \qquad (x, x'') = -1. \tag{5.5}$$

Let $y = x + \alpha x''$ where α is a scalar. We seek a value for α for which $(x, y) = 0$. Since

$$(x, y) = (x, x) + \alpha(x, x'') = 1 - \alpha,$$

we obtain $\alpha = 1$. Therefore $y = x + x''$, and y is consequently orthogonal to x and to x'. Now

$$N(y) = (x + x'', x + x'') = (x, x) + 2(x, x'') + (x'', x'') = (x'', x'') - 1 \neq 0.$$

Let

$$\xi_3 = \frac{x + x''}{[(x'', x'') - 1]^{\frac{1}{2}}}. \tag{5.6}$$

Thus ξ_3 is a normalized quaternion that represents a lineal element orthogonal to ξ_1 and to ξ_2.

Let z be the pole of the planar field determined by the linearly independent lineal elements x, x' and y. Then

$$(x, z) = (x', z) = (y, z) = 0.$$

Since $(y, z) = (x, z) + (x'', z)$, we get $(x'', z) = 0$. Therefore

$$z = \begin{Vmatrix} x_0 & x_1 & x_2 & x_3 \\ x_0' & x_1' & x_2' & x_3' \\ x_0'' & x_1'' & x_2'' & x_3'' \end{Vmatrix} \tag{5.7}$$

and

$$N(z) = \begin{vmatrix} (x, x) & (x, x') & (x, x'') \\ (x', x) & (x', x') & (x', x'') \\ (x'', x) & (x'', x') & (x'', x'') \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & (x'', x'') \end{vmatrix} = (x'', x'') - 1.$$

Let

$$\xi_4 = \frac{z}{[(x'', x'') - 1]^{\frac{1}{2}}}. \tag{5.8}$$

Thus ξ_4 is a normalized quaternion representing a lineal element orthogonal to the lineal elements ξ_1, ξ_2, and ξ_3.

Let $\mathfrak{d}$ represent the determinant of the components of the four ξ_i. Then

$$\mathfrak{d}^2 = |(\xi_i, \xi_j)| = 1.$$

Consequently the four normalized quaternions ξ_i are linearly independent. They therefore constitute a linear basis for arbitrary quaternions. Hence we can set the four quaternions $\xi_i'(= d\xi_i/d\sigma)$ equal to the linear combinations

$$\xi_i' = a_{i1}\xi_1 + a_{i2}\xi_2 + a_{i3}\xi_3 + a_{i4}\xi_4 \qquad (i = 1, 2, 3, 4). \tag{5.9}$$

Since $(\xi_i, \xi_j) = \delta_{ij}$, we obtain

$$(\xi_i, \xi_j') + (\xi_i', \xi_j) = 0. \tag{5.10}$$

Scalar multiplication of the equations (5.9) by the ξ_j yields

$$a_{ij} = (\xi_i', \xi_j) = -(\xi_i, \xi_j') = -a_{ji}.$$

Therefore the matrix $||a_{ij}||$ is skew-symmetric. Furthermore, since $\xi_1' = \xi_2$, we find that

$$a_{12} = 1, \qquad a_{13} = a_{14} = 0.$$

Let

$$\frac{1}{\rho} = [(x'', x'') - 1]^{\frac{1}{2}}. \tag{5.11}$$

Then (5.4) and (5.5) yield

$$\xi_2' = -\xi_1 + \frac{1}{\rho}\xi_3.$$

Consequently

$$a_{23} = (\xi_2', \xi_3) = \frac{1}{\rho} \quad \text{and} \quad a_{24} = 0.$$

It remains to find the value of $a_{34} = (\xi_3', \xi_4) = -(\xi_4', \xi_3)$. Since

$$\xi_3 = \rho(x + x''),$$

$$\xi_3' = \rho' x + \rho' x'' + \rho x' + \rho x'''.$$

Scalar multiplication of ξ_3' by $\xi_4 = \rho z$ yields

$$(\xi_3', \xi_4) = \rho\rho'(x, z) + \rho^2(x', z) + \rho\rho'(x'', z) + \rho^2(x''', z).$$

But z is orthogonal to x, x' and x''; therefore

$$(\xi_1', \xi_4) = \rho^2(x''', z) = \frac{\Delta}{1 - (x'', x'')} \tag{5.12}$$

where

$$\Delta = \begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ x_0' & x_1' & x_2' & x_3' \\ x_0'' & x_1'' & x_2'' & x_3'' \\ x_0''' & x_1''' & x_2''' & x_3''' \end{vmatrix}. \tag{5.13}$$

Let

$$\frac{1}{\tau} = \frac{\Delta}{1 - (x'', x'')}. \tag{5.14}$$

Then the system of equations (5.9) reduces to the following:

$$\begin{aligned} \xi_1' &= \xi_3 \\ \xi_2' &= -\xi_1 + \frac{1}{\rho}\xi_3 \\ \xi_3' &= -\frac{1}{\rho}\xi_2 + \frac{1}{\tau}\xi_4 \\ \xi_4' &= -\frac{1}{\tau}\xi_3 \end{aligned} \tag{5.9*}$$

This system of equations is the analogue for a series $\mathfrak{S}$ under $\mathfrak{G}_6$ of the Serret-Frenet formulae for a curve in Euclidean space. We shall call $1/\rho$ and $1/\tau$ the $\mathfrak{G}_6$-*curvature* and $\mathfrak{G}_6$-*torsion* of $\mathfrak{S}$ respectively. Given two arbitrary functions $\rho(\sigma)$ and $\tau(\sigma)$, a series is determined within a whirl-rotation by means of (5.9*). We can therefore regard $\rho = \rho(\sigma)$ and $\tau = \tau(\sigma)$ as the intrinsic equations of a series relative to $\mathfrak{G}_6$.

If $\mathfrak{S}$ is a turbine, its parametric equation (see (2.8)) may be expressed in the form

$$x = q(-\cos t + r \sin t), \quad q\bar{q} = 1, \quad r^2 = -1,$$

where q and r are constant quaternions. Since $(dx/dt)\,(d\bar{x}/dt) = 1$, $t = \pm\sigma$ + const. Consequently, if $x(t)$ is a turbine,

$$(x', x') = 1 \quad \text{and} \quad (x'', x'') - 1 = 0$$

where x' and x'' denote differentiation with respect to σ. Conversely, it can be shown that a series $\mathfrak{S}: x(\sigma)$, such that

$$N(y) = (x'', x'') - 1 = 0, \tag{5.15}$$

is a turbine. For (5.15) implies that $y = x'' + x = 0$. Therefore $\bar{x}x'' + \bar{x}x = 0$. Consequently $\bar{x}x'' = -1$. But the fixed centrode of $\mathfrak{S}$, namely $\pm Z = \pm \bar{x}x'$. Therefore

$$\frac{dZ}{d\sigma} = \bar{x}x'' + \bar{x}'x' = 0,$$

which implies that the fixed centrode of $\mathfrak{S}$ is a pair of diametrically opposite points and consequently, that $\mathfrak{S}$ is a turbine. Thus (5.15) is a necessary and sufficient condition that a series be a turbine; or, what is equivalent, a necessary and sufficient condition that $\mathfrak{S}$ be a turbine is that $1/\rho = 0$. Torsion is not defined for turbines.

Reverting to the original parameter t, we find the following expressions for the differential invariants:

$$\frac{1}{\rho^2} = \omega \Big/ \left(\frac{dx}{dt}, \frac{dx}{dt}\right)^3 \tag{5.11*}$$

and

$$\frac{1}{\tau} = -\frac{\Delta_1}{\omega} \tag{5.14*}$$

where

$$\omega = \left(\frac{dx}{dt}, \frac{dx}{dt}\right)\left(\frac{d^2x}{dt^2}, \frac{d^2}{dt^2}\right) - \left(\frac{dx}{dt}, \frac{d^2x}{dt^2}\right)^2 - \left(\frac{dx}{dt}, \frac{dx}{dt}\right)^3,$$

$$\Delta_1 = \left| x_0, \frac{dx_1}{dt}, \frac{d^2x_2}{dt^2}, \frac{d^3x_3}{dt^3} \right|.$$

6. Kinematic and non-Euclidean interpretations of the differential invariants ρ and τ. Let the displacement $\mathcal{M}$, defined by a series $\mathfrak{S}: x(\sigma)$, have $\pm Z(\sigma) = \pm \bar{x}x'$ for its fixed centrode. We assume that $\mathfrak{S}$ is not a turbine, that is, that $(x'', x'') - 1 \neq 0$. Let the unit vector

$$\xi_1 = \bar{x}x' \tag{6.1}$$

have its initial point at O, the centre of the fixed sphere S_f. Let s be the Euclidean arc-length of the fixed centrode $Z(\sigma)$ measured from σ_0 to σ. Then

$$ds^2 = (Z', Z')d\sigma^2 = (\xi_1', \xi_1')d\sigma^2.$$

But $Z' = \bar{x}x'' + \bar{x}'x' = 1 + \bar{x}x''$. Therefore

$$ds^2 = [(x'', x'') - 1]\, d\sigma^2 = \frac{1}{\rho^2} d\sigma^2.$$

We orient $Z(\sigma)$ so that $ds/d\sigma = 1/\rho > 0$. Now

$$\frac{d\zeta_1}{ds} = (\bar{x}x'' + \bar{x}'x')\frac{d\sigma}{ds} = \rho\bar{x}(x'' + x).$$

Let

$$\zeta_2 = \frac{d\zeta_1}{ds} = \rho\bar{x}(x'' + x). \tag{6.2}$$

Evidently ζ_2 is a unit vector tangent to the fixed centrode at the point σ.

Let ζ_3 be the vector product of ζ_1 and ζ_2. Then

$$\zeta_3 = \zeta_1 \times \zeta_2 = \zeta_1\zeta_2. \tag{6.3}$$

Therefore ζ_3 is a unit vector tangent to S_f and orthogonal to ζ_1 and ζ_2. The three orthogonal unit vectors ζ_i constitute a moving trihedral of the fixed centrode considered as a spherical curve. The vectors ζ'_i $(i = 1,2,3)$ being linearly dependent on the ζ_i, we can let

$$\zeta'_i = \beta_{i1}\zeta_1 + \beta_{i2}\zeta_2 + \beta_{i3}\zeta_3 \qquad (i = 1, 2, 3;\ \beta_{ij} \text{ real scalars}). \tag{6.4}$$

Evidently the (Euclidean) scalar product $\zeta_i \cdot \zeta_j$ of the vectors ζ_i, ζ_j is equal to (ζ_i, ζ_j). Since $\zeta_i \cdot \zeta_j = \delta_{ij}$,

$$\zeta_i\zeta'_j + \zeta'_i\zeta_j = 0.$$

Hence $||\beta_{ij}||$ is skew-symmetric. From (6.2) we obtain

$$\beta_{12} = -\beta_{21} = \frac{1}{\rho}.$$

We proceed to evaluate $\beta_{23} = \zeta'_2 \cdot \zeta_3 = (\zeta'_2, \zeta_3)$. Since ζ_1 and ζ_2 are orthogonal vectors, (6.1), (6.2), and (6.3) yield

$$\zeta_3 = \zeta_1\zeta_2 = \rho x\bar{x}'\bar{x}(x'' + x).$$

Observing that $\bar{x}x'\bar{x}x' = -1$, we obtain

$$\zeta_3 = -\rho(\bar{x}'x'' + \bar{x}'x).$$

Moreover,

$$\zeta'_2 = \rho'\bar{x}(x'' + x) + \rho(\bar{x}'x'' + \bar{x}x''')$$

and, since $(\zeta_2, \zeta_3) = 0$,

$$\zeta'_2 \cdot \zeta_3 = (\zeta'_2, \zeta_3) = \rho(\bar{x}'x'' + \bar{x}x''', \zeta_3).$$

This can be reduced, by virtue of (2.4), (5.2), and (5.11), to

$$-1 - \rho^2[(\bar{x}x''', \bar{x}'x'') + (\bar{x}x''', \bar{x}'x)].$$

To evaluate the scalar products in the square brackets, write

$$p_{ij} = x_ix_j''' - x_jx_i''', \quad q_{ij} = x'_ix''_j - x'_jx''_i, \quad t_{ij} = x'_ix_j - x'_jx_i.$$

Observing that, by reason of (5.5), $(x, x''') = 0$, we obtain

$$\bar{x}x''' = e_1(p_{01} - p_{23}) + e_2(p_{02} - p_{31}) + e_3(p_{03} - p_{12}),$$
$$\bar{x}'x'' = e_1(q_{01} - q_{23}) + e_2(q_{02} - q_{31}) + e_3(q_{03} - q_{12}).$$

Therefore

$$(\bar{x}x''', \bar{x}'x'') = \sum p_{ij}q_{ij} - \sum p_{ij}q_{kl},$$

where i,j and k,l are complementary pairs of subscripts. But

$$\sum p_{ij}q_{ij} = \begin{vmatrix} (x, x') & (x, x'') \\ (x''', x')(x''', x'') \end{vmatrix} = \begin{vmatrix} 0 & -1 \\ -(x'', x'')(x''', x'') \end{vmatrix} = -(x'', x'')$$

and

$$\sum p_{ij}q_{kl} = \Delta.$$

Therefore

$$(\bar{x}x''', \bar{x}'x'') = -(x'', x'') - \Delta.$$

Similarly

$$(\bar{x}x''', \bar{x}'x) = \sum p_{ij}p'_{ij} - \sum p_{ij}p'_{kl}.$$

But

$$\sum p_{ij}p'_{ij} = \begin{vmatrix} (x, x') & (x, x) \\ (x''', x')(x''', x') \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ -(x'', x'') & 0 \end{vmatrix} = (x'', x'')$$

and

$$\sum p_{ij}p'_{kl} = 0.$$

Hence $(\bar{x}x''', \bar{x}'x) = (x'', x'')$. Consequently

$$\beta_{22} = -\beta_{32} = \rho^2\Delta - 1 = -1 - \frac{1}{\tau}.$$

Substituting the expressions we have found for the β_{ij} in (6.4), we obtain

$$\begin{aligned} \zeta'_1 &= \frac{1}{\rho}\zeta_2 \\ \zeta'_2 &= -\frac{1}{\rho}\zeta_1 - \left(1 + \frac{1}{\tau}\right)\zeta_3 \\ \zeta'_3 &= \left(1 + \frac{1}{\tau}\right)\zeta_2 \end{aligned} \tag{6.4*}$$

If we change from the parameter σ to s (Euclidean arc-length), the system (6.4*) becomes

$$\begin{aligned} \frac{d\zeta_1}{ds} &= \zeta_2 \\ \frac{d\zeta_2}{ds} &= -\zeta_1 - \rho\left(1 + \frac{1}{\tau}\right)\zeta_3 \\ \frac{d\zeta_3}{ds} &= \rho\left(1 + \frac{1}{\tau}\right)\zeta_2 \end{aligned} \tag{6.4**}$$

The system (6.4**) is the set of Serret-Frenet formulae of $Z(s)$ regarded as a spherical curve.

Evidently $K_f = -\rho(1 + 1/\tau)$ is the geodesic curvature of the fixed centrode, and represents the rate of turning (bending) of the plane tangent to the fixed (space) cone as its point of tangency with the fixed centrode moves on it with unit speed. If R is the radius of curvature of $Z(s)$ regarded as a space curve, $R^{-2} = K_f^2 + 1$.

In a similar manner, the Serret-Frenet formulae for the mobile centrode $\pm W(\sigma)$ on S_m can be found. Letting η_1 be the unit vector $W(\sigma) = x'\bar{x}$ at the point σ, η_2 the unit vector tangent to $W(\sigma)$ at σ, and $\eta_3 = \eta_1 \times \eta_2 = \eta_1\eta_2$, we obtain

$$
(6.5)\qquad
\begin{aligned}
\frac{d\eta_1}{ds} &= \qquad\qquad \eta_2 \\
\frac{d\eta_2}{ds} &= -\eta_1 \qquad\qquad + \rho\left(1 - \frac{1}{\tau}\right)\eta_3 \\
\frac{d\eta_3}{ds} &= \qquad -\rho\left(1 - \frac{1}{\tau}\right)\eta_2
\end{aligned}
$$

where s is the Euclidean arc-length of the mobile centrode. The geodesic curvature of the mobile centrode is $K_m = \rho(1 - 1/\tau)$.

The geodesic curvatures $K_f(s)$ and $K_m(s)$ determine the fixed and mobile centrodes on S_f and S_m respectively within rotations around O. Hence the differential invariants $\rho(\sigma)$ and $\tau(\sigma)$ which determine a series $\mathfrak{S}$ within a whirl-rotation also determine, within rotations, the fixed and mobile centrodes of the continuous motion $\mathscr{M}$ defined by $\mathfrak{S}$. When K_f and K_m are constant, the two centrodes are circles, and the motion $\mathscr{M}$ becomes that of a circle of radius $(1 + K_m^2)^{-\frac{1}{2}}$ on S_m rolling without slipping on a circle of radius $(1 + K_f^2)^{-\frac{1}{2}}$ on S_f.

If we regard the four components x_1 of the quaternion x as the homogeneous coordinates of a point in projective three-space, we obtain a continuous one-to-one mapping of the lineal elements x on S upon the points x in three-space. By virtue of this mapping it is evident that to the ∞^6 whirl-rotations (2.3) on S correspond the ∞^6 displacements in elliptic space E_3; indeed, to the whirls correspond the left-translations in E_3 and to the rotations correspond the right-translations. A series $\mathfrak{S}$ as in (5.1) is mapped on a curve $\mathscr{C}$ in E_3, turbines being mapped on the straight lines. If $\mathfrak{S}$ is not a turbine, the moving frame of lineal elements ξ_i $(i = 1,2,3,4)$ associated with $\mathfrak{S}$ is mapped on a frame of four points associated with $\mathscr{C}$. The invariants $1/\rho$ and $1/\tau$ can be interpreted as the elliptic curvature and torsion respectively of $\mathscr{C}$, and the equations (5.9*) become the Serret-Frenet formulae for a curve in E_3. A continuous motion of S_m over S_f which corresponds within a whirl-rotation to a series $\mathfrak{S}$ on S therefore also corresponds within an elliptic displacement to a curve $\mathscr{C}$ in E_3.

References

1. W. Blaschke, *Euklidische Kinematik und nichteuklidische Geometrie*, Z. Math. Phys., vol. 60 (1911), 61-91 and 203-204.
2. ———, *Ebene Kinematik* (Leipzig and Berlin, 1938).
3. J. DeCicco, *The geometry of whirl series*, Trans. Amer. Math. Soc., vol. 43 (1938), 344-358.
4. ———, *The differential geometry of series of lineal elements*, Trans. Amer. Math. Soc., vol. 46 (1939), 348-361.
5. J. M. Feld, *The geometry of whirls and whirl-motions in space*, Bull. Amer. Math. Soc., vol. 47 (1941), 927-933.
6. ———, *Whirl-similitudes, Euclidean kinematics, and non-Euclidean geometry*, Bull. Amer. Math. Soc., vol. 48 (1942), 783-790.
7. ———, *On a representation in space of groups of circle and turbine transformations in the plane*, Bull. Amer. Math. Soc., vol. 50 (1944), 930-934.
8. ———, *A kinematic characterization of series of lineal elements in the plane and of their differential invariants under the group of whirl-similitudes and some of its subgroups*, Amer. J. Math., vol. 70 (1948), 129-138.
9. J. Grünwald, *Ein Abbildungsprinzip, welches die ebene Geometrie und Kinematik mit der räumlichen Geometrie verknüpft*, S.B. Akad. Wiss. Wien., IIa, vol. 80 (1911), 677-741.
10. E. Kasner, *The group of turns and slides and the geometry of turbines*, Amer. J. Math., vol. 33 (1911), 193-202.
11. E. Kasner and J. DeCicco, *The geometry of turbines, flat fields and differential equations*, Amer. J. Math., vol. 59 (1937), 545-563.
12. ———, *The geometry of the whirl-motion group G_6: elementary invariants*, Bull. Amer. Math. Soc., vol. 43 (1937), 399-403.
13. A. Narasinga Rao, *Studies in turbine geometry* I, J. Indian Math. Soc., vol. 3 (1938), 96-108; II, Proc. Indian Acad. Sc., vol. 8A (1938), 179-186.
14. G. Scheffers, *Isogonalkurven, Aequitangentialkurven und komplexe Zahlen*, Math. Ann., vol. 60 (1905), 491-531.
15. K. Strubecker, *Zur Geometrie sphärischer Kurvenscharen*, Jber. dtsch. MatVer., vol. 44 (1934), 184-198.

Queens College
Flushing, N.Y.

ON THE PROPERTY C AND A PROBLEM OF HAUSDORFF

FRITZ ROTHBERGER

1. Introduction. In an earlier paper [3] I studied the property C and related properties C′ and C″; but the principal problem, viz, to prove, with the axiom of choice only (without any other hypothesis), the existence of a non-denumerable set of property C, remains open.

In another paper [4] I studied Hausdorff's problem [1] of the existence of Ω-limits for (transfinite) sequences of dyadic sequences, and we have some conditional results; but again the main problem remains open, viz, the problem of proving (with the axiom of choice only) the existence of such Ω-limits.

In the present paper we are going to solve, in a certain sense, a compound of these two problems. We are going to show that: either there exist Ω-limits, or non-denumerable C-sets, or both (Theorem I). We also prove two other theorems which are related.

For the definitions and the general theory we refer the reader to the two papers mentioned above. We shall, however, repeat here those theorems which we are going to use explicitly, and those definitions where more than just the name occurs.

We denote generically a finite set by Λ. Individual finite sets will be indicated with a superscript, such as Λ^1, Λ^a. If $E \subset F + \Lambda$, we shall write $E < F$ (E is almost-contained in F). Whereas, in [4], these definitions were used for sets of natural numbers only, we shall use them here for other sets also, but only for subsets of a fixed denumerable set (e.g., the set of all rational numbers) and thus we shall still have the same theorems, *mutatis mutandis*.

A set E is said to have the property C″ if every double sequence of intervals J_{mn} satisfying the conditions

$$E \subset \sum_n J_{mn} \quad \text{(for all } m\text{)},$$

contains a diagonal sequence

$$J_{1n_1}, J_{2n_2}, \ldots, J_{mn_m}, \ldots$$

such that

$$E \subset \sum_m J_{mn_m}.$$

It can easily be shown that *every* C″-set is a C-set [cf. 2].

THEOREM I. *The non-existence of Ω-limits (for dyadic sequences) implies that every linear set of power* $\aleph_1$ *has property* C *(and also* C″*).*

Received June 20, 1950.

We shall actually prove it for $\mathbf{C}''$ and we shall give two proofs.

THEOREM II. *The non-existence of Ω-limits implies the following proposition: Given any family of $\aleph_1$ infinite sets of natural numbers E^α ($\alpha < \Omega$), there exists a set D such that $E^\alpha \cdot D$ and $E^\alpha \cdot CD$ are infinite sets, for all α.* (CD means: complement of D.)

There is a stronger theorem, from which the above two follow, namely:

THEOREM III. *The non-existence of Ω-limits implies the following proposition: The sum of $\aleph_1$ (linear) sets of first category is again of first category.*

For the proofs of these theorems we need a few preliminaries.

The abbreviation "of n.n." means "of natural numbers." The letters μ, ν, m, n, r, s, t, (without or with subscripts) will always denote natural numbers; and the letters a, b, c, d, (without or with subscripts) will denote "segments," to be defined presently. Sets of segments, and also other sets, will be denoted by capitals, A, B, ...

A finite sequence of n.n. $(r_1, r_2, \ldots, r_n)$ will be called a *segment*. The first m terms ($m < n$) of a segment form a *subsegment*. Example: (1, 3, 5) is a subsegment of (1, 3, 5, 7, 9), but (1, 5, 9) is not a subsegment of it in our sense.

The word "sequence" shall always mean "infinite sequence."

Two sequences of n.n., $\{s_n\}$ and $\{t_n\}$, will be said to *intersect* if we have $s_n = t_n$ for some value of n. (In [3, p. 118, Lemme 5], two sequences were said to be "tout-à-fait différentes" if and only if, in this sense, they do not intersect.)

A sequence s_n and a segment $(r_1, r_2, \ldots, r_m)$ *intersect*, if $s_n = r_n$ for some $n \leqslant m$.

For a given set $\mathscr{S}$ of sequences of n.n., a *diagonal sequence* is a sequence (not necessarily in $\mathscr{S}$) which intersects each element of $\mathscr{S}$. If such a sequence exists, we shall say that $\mathscr{S}$ *admits a diagonal*.

We quote five theorems from the other papers, for later use:

(1) [3, p. 119, Lemme 6]. *The proposition 'Every linear set of power $\aleph_1$ has property $\mathbf{C}''$' is equivalent to the following: 'Every set of sequences (of* n.n.*) of power $\aleph_1$ admits a diagonal.'*

(2) [3, p. 120, Lemme 8]. *The existence of a non-$\mathbf{C}''$ set of power $\aleph_1$ implies that the interval* (0, 1) *is the sum of $\aleph_1$ sets of first category.*

(3) [4, p. 34, Theorem 3$^\alpha$]. *The non-existence of Ω-limits implies the proposition $\mathbf{B}(\aleph_1)$, i.e., the non-existence of (Ω, ω^*)-gaps.*

(4) [4, p. 37, Lemma 5]. *$\mathbf{B}(\aleph_1)$ is equivalent to the following proposition: 'If $Y_n < X_\alpha$ for all $n < \omega$, $\alpha < \Omega$ (X's and Y's are sets of* n.n.*), then there exists a set D such that $Y_n < D < X_\alpha$ for all n and α.'*

(5) [4, p. 38, Lemma 7]. *The non-existence of Ω-limits (for dyadic sequences) implies the following proposition: 'Given $\aleph_1$ sets (of* n.n.*) X_α, if every finite product of X's is an infinite set, then there exists an infinite set D, such that $D < X_\alpha$ (for all α).'* ("Finite product" means a product of a finite number of sets.)

The last two theorems, i.e., (4) and (5), are the clue to the proofs of this paper; they also contain, in a sense, the clue to [4, Chapter III]. We shall, however, have to replace, in (4) and (5), the words "of n.n." by "of segments" and later on by "of rational numbers." This is permissible, since, in theorems of this type, the set of all natural numbers may be replaced by any other denumerable set, e.g., the set of all segments.

(4′), (5′). Same as (4), (5), with "segments" or "rational numbers" in place of "n.n."

2. Proof of Theorem I. We need the following two new lemmas, which are obvious:

LEMMA (i). *Given a finite set of sequences (of* n.n.*), there exist infinitely many diagonal segments, a diagonal segment being a segment intersecting each of the given sequences.*

LEMMA (ii). *Given a segment* $b = (r_1, r_2, \ldots, r_m)$ *and a finite set of sequences, there exist infinitely many diagonal segments starting with* $(r_1, r_2, \ldots, r_m)$, *i.e., having* b *as a subsegment.*

Proof of Theorem I. Let

$$\{s_n^1\}, \{s_n^2\}, \ldots, \{s_n^\omega\}, \ldots, \{s_n^\alpha\}, \ldots \qquad (\alpha < \Omega)$$

be a fixed, but arbitrary, set of $\aleph_1$ sequences of n.n.

Assuming that no Ω-limits exist, it is sufficient to show that the above set admits a diagonal sequence, cf. (1).

Let A^α be the set of all segments intersecting $\{s_n^\alpha\}$. It follows from Lemma (i) that every finite product

$$\prod_{\nu=1}^{n} A^{\alpha_\nu}$$

is an infinite set, hence, by (5′), there exists an infinite set (of segments) D_0 such that $D_0 < A^\alpha$ (all $\alpha < \Omega$).

More generally, let A_b^α be the set of all those segments which have b as a (proper) subsegment and intersect $\{s_n^\alpha\}$. Just as before, but using Lemma (ii), we see that every finite product is an infinite set, hence there exists an infinite set D_b, such that $D_b < A_b^\alpha$ (all α).

Since obviously $A_b^\alpha < A^\alpha$, we have $D_b < A^\alpha$, for all α and all segments b. Now, the b's form a denumerable set, and the α's a set of power $\aleph_1$, hence, by (3) and (4′), there exists a set D such that

$$D_b < D < A^\alpha, \quad \text{for all } \alpha \text{ and all } b. \tag{6}$$

We shall use this set D to construct the required diagonal sequence.

Let $b_1 \in D$. Next, let

$$b_2 \in D_{b_1} \cdot D.$$

(Such a segment exists, because $D_b \cdot D$ is an infinite set for any b.) Note that b_1 is a subsegment of b_2. Next, let

$$b_2 \in D_{b_1} \cdot D,$$

and, generally, let

$$b_{n+1} \in D_{b_n} \cdot D, \ldots .$$

We see that b_n is always a (proper) subsegment of b_{n+1}, hence all b_n's are subsegments of one common sequence. More explicitly, we can write:

$$b_1 = (r_1, r_2, \ldots, r_{\nu_1}),$$

$$b_2 = (r_1, r_2, \ldots, r_{\nu_1}, \ldots, r_{\nu_2}),$$

$$\ldots \qquad \ldots$$

$$b_n = (r_1, r_2, \ldots, r_{\nu_1}, \ldots, r_{\nu_2}, \ldots, r_{\nu_n}),$$

$$\ldots \qquad \ldots$$

In order to show that $\{r_n\}$ is the required diagonal sequence, it is sufficient to notice that, by definition, $b_n \in D$ for all n, and that, by (6), $D < A^\alpha$ for all α. Thus $b_n \in A^\alpha$ for any given α and almost all n. Therefore, for any given α, almost all b_n intersect $\{s_n^\alpha\}$, and hence $\{r_n\}$ intersects $\{s_n^\alpha\}$ for all α.

Theorem II can be proved in a similar way, but we shall rather deduce it from Theorem III.

3. Proof of Theorem III. We need the following result:

(7) [3, p. 112, Théorème 1,B_3]. $\mathbf{B}(\aleph_1)$ *is equivalent to the following proposition: 'The sum of* $\aleph_1 F_\sigma$*'s disjoint from* $\mathfrak{R}$ *is contained in an* F_σ *disjoint from* $\mathfrak{R}$*, where* $\mathfrak{R}$ *is the set of all rational numbers.'*

Now, the set $\mathfrak{R}$ may be replaced by any other dense denumerable set $\mathfrak{D}$; also, the sum of $\aleph_1 F_\sigma$'s is equal to the sum of $\aleph_1$ closed sets (because $\aleph_1 \cdot \aleph_0 = \aleph_1$). From this, together with (3) and (7), we have the following:

LEMMA (iii). *The non-existence of* Ω*-limits implies the proposition: 'The sum of* $\aleph_1$ *closed sets disjoint from* $\mathfrak{D}$*, is contained in an* F_σ *disjoint from* $\mathfrak{D}$*; where* $\mathfrak{D}$ *is any everywhere-dense denumerable set.'*

Taking complements, we get the following:

LEMMA (iv). *The non-existence of* Ω*-limits implies that the product of* $\aleph_1$ *open sets or* G_δ*'s containing* $\mathfrak{D}$*, contains a* G_δ *containing* $\mathfrak{D}$ *(where* $\mathfrak{D}$ *is everywhere dense and denumerable).*

Proof of Theorem III. Without loss of generality, the sets of first category in the proposition in the theorem may be replaced by F_σ's of first category, i.e., by non-dense F_σ's. Then, by the same argument as above, the proposition may be changed to the following one:

The product of $\aleph_1$ *everywhere-dense open sets contains an everywhere-dense* G_δ.

Let $G^1, G^2, \ldots, G^\omega, \ldots, G^\alpha, \ldots$ $(\alpha < \Omega)$ be $\aleph_1$ everywhere-dense open sets. It is sufficient to prove that they contain an everywhere-dense G_δ, assuming the non-existence of Ω-limits.

Let A^α be the set of all rational numbers contained in G^α. Since every finite product of G^α's is again an open set, every finite product of A^α's is an infinite set. Hence, by (5′), there exists an infinite set D_0 with $D_0 < A^\alpha$ (for all α).

Now let J be any interval with rational endpoints. Then $J \cdot A^\alpha$ is the set of rational points in $J \cdot G^\alpha$. Again, any finite product of these sets $J \cdot A^\alpha$ is an infinite set. Hence there is an infinite set D_J with $D_J < J \cdot A^\alpha < A^\alpha$, for all α. Thus we have:

(8) $D_J \subset J$, for all J's,

(9) $D_J < A^\alpha$, for any J and any α. (There are $\aleph_0$ J's and $\aleph_1$ α's.)

Therefore, by (3), (4′), and (9), there is a set D with $D_J < D < A^\alpha$, for all J and α.

Now, since D_J is an infinite set, it has, by (8), at least one accumulation point in the closure of J, and this accumulation point is necessarily an accumulation point of D, because almost all[1] elements of D_J are elements of D. Thus we see that D has accumulation points in every interval J, therefore D is everywhere-dense (and denumerable).

Also, since $D < A^\alpha$, we have $D \subset A^\alpha + \Lambda^\alpha$, where the Λ^α's are certain subsets of $\mathfrak{R}$; and since $A^\alpha \subset G^\alpha$, we finally have

(10) $$D \subset G^\alpha + \Lambda^\alpha, \quad \text{for all } \alpha.$$

We may now apply Lemma (iv), for the left hand side of (10) is everywhere-dense and denumerable, whereas the right hand side is a G_δ (because the sum of an open set and a finite set is always a G_δ).

It follows, from Lemma (iv), that there exists a G_δ, say E, such that

(11) $$D \subset E \subset \prod_\alpha (G^\alpha + \Lambda^\alpha) \subset \prod_\alpha G^\alpha + \mathfrak{R}.$$

From $D \subset E$ it follows that E is everywhere-dense, therefore it is everywhere of second category (because it is a G_δ). Therefore, $E - \mathfrak{R}$ is still everywhere-dense and is obviously still a G_δ. Finally, we see from (11), that $E - \mathfrak{R}$ is contained in all G^α. Thus $E - \mathfrak{R}$ is the G_δ which we set out to find.

4. Proof of Theorem II. To every set of n.n. there corresponds a dyadic "decimal" representation of a real number belonging to the interval [0,1]. A set of sets of n.n. is said to be non-dense, or of first category, if the corresponding set of real numbers is non-dense, or of first category. Let E be an infinite set of n.n. Then the linear set corresponding to the set of X's such that $E \subset X$ is a Cantor discontinuum, and thus non-dense, and the set of X's such that $E < X$ is of first category, being the sum of $\aleph_0$ non-dense sets.

[1] "almost all" means "all but a finite number of."

Similarly, the set of all X's such that $E < CX$ is also of first category. Hence, the set of all X's such that

(12) $$\text{either } E \cdot X = \Lambda \text{ or } E \cdot CX = \Lambda,$$

is of first category. Therefore, given a set of $\aleph_1$ infinite sets E^α ($\alpha < \Omega$), and assuming that there are no Ω-limits, it follows from Theorem III that the set of all X's such that

(13) $$\text{for } \textit{some } \alpha, \text{ either } E^\alpha \cdot X = \Lambda \text{ or } E^\alpha \cdot CX = \Lambda,$$

is likewise of first category. Hence the complement of this set of X's is not empty (because of second category), so that there exists an infinite set D (belonging to the said complement and thus satisfying the negation of (13)), such that

(14) $$\text{for } \textit{all } \alpha, \text{ both } E^\alpha \cdot D \text{ and } E^\alpha \cdot CD \text{ are infinite sets,}$$

which proves the theorem.

5. Alternative proof of Theorem I. It follows from (2) (reversing the implication) that, if the sum of $\aleph_1$ sets of first category is always also of first category, then every set of power $\aleph_1$ has property C″. Combining this with Theorem III, we have our theorem.

References

1. F. Hausdorff, *Summen von $\aleph_1$ Mengen*, Fund. Math., vol. 26 (1936), 247.
2. F. Rothberger, *Eine Verschärfung der Eigenschaft* C, Fund. Math., vol. 30 (1938), 54.
3. F. Rothberger, *Sur les familles indénombrables de suites de nombres naturels et les problèmes concernant la propriété* C, Proc. Cambridge Philos. Soc., vol. 37 (1941), 109-126.
4. F. Rothberger, *On some problems of Hausdorff and of Sierpiński*, Fund. Math., vol. 35 (1948), 29-46.

University of New Brunswick

A REMARK ON THE EXISTENCE OF A DENUMERABLE BASE FOR A FAMILY OF FUNCTIONS

FRITZ ROTHBERGER

A family F of functions is said to have a *denumerable base* if there exists a sequence of functions $\{f_n(x)\}$ (not necessarily $\in F$) such that any function $f \in F$ is the limit of a subsequence of $\{f_n(x)\}$. The *domain* X of a function $f(x)$ is the set of x's for which $f(x)$ is defined; we say $f(x)$ is a *function on* X. A *dyadic function* is a function taking only the values 0 and 1.

Let F be a family of dyadic functions on a set X.

PROPOSITION $(\mathfrak{m}, \mathfrak{n})$. *If* $\bar{\bar{F}} = \mathfrak{m}$ *and* $\bar{\bar{X}} = \mathfrak{n}$, *then the family* F *has a denumerable base.*

In an earlier paper I have shown that the proposition $(\aleph_1, \aleph_1)$ is true [1, p. 401, Theorem 3]. Hence, the continuum hypothesis implies the proposition $(\mathfrak{c}, \mathfrak{c})$ [*ibid.*, Corollary].

The problem is whether or not the proposition $(\mathfrak{c}, \mathfrak{c})$ can be proved independently (i.e., merely with the axiom of choice, but without any additional hypothesis such as the continuum hypothesis). We are going to prove a theorem which throws some light on this problem.

First, we need two lemmas (proofs omitted):

LEMMA A. *If* $\mathfrak{n}_1 > \mathfrak{n}_2$, *then proposition* $(\mathfrak{m}, \mathfrak{n}_1)$ *implies proposition* $(\mathfrak{m}, \mathfrak{n}_2)$.

LEMMA B. *If* $\aleph_\alpha < \mathfrak{c}$, *then proposition* $(\mathfrak{c}, \mathfrak{c})$ *implies proposition* $(\mathfrak{c}, \aleph_\alpha)$.

These will enable us to prove the following

THEOREM. *If there exists an* α *and a* β *such that*

$$\aleph_\alpha < \aleph_\beta, \quad \aleph_\beta \leqslant \mathfrak{c} < \aleph_{\omega_\beta}, \quad 2^{\aleph_\alpha} = \aleph_{\omega_\beta}, \tag{1}$$

then the proposition $(\mathfrak{c}, \aleph_\alpha)$ *is false.*

For example,

$$\alpha = 1, \beta = 2, \aleph_2 \leqslant \mathfrak{c} < \aleph_{\omega_2} = 2^{\aleph_1}.$$

Incidentally, the first relation in (1) is redundant: it follows from the third one by Koenig's theorem.

From this theorem, together with Lemma B, we have:

COROLLARY 1. *If* $\aleph_\alpha$, $\aleph_\beta$ *satisfying* (1) *exist, the proposition* $(\mathfrak{c}, \mathfrak{c})$ *is false.*

We have, in particular (special cases):

Received June 20, 1950.

COROLLARY 2. *The proposition* $(\mathfrak{c}, \mathfrak{c})$ *is false if any one of the following propositions* (2), (3), (4), *holds:*

(2) $$2^{\aleph_1} = \aleph_{\omega_2} \text{ and } \aleph_2 < \mathfrak{c} < \aleph_{\omega_2};$$

(3) $$2^{\aleph_2} = \aleph_{\omega_3} \text{ and } \aleph_3 < \mathfrak{c} < \aleph_{\omega_3};$$

(4) $$2^{\aleph_n} = \aleph_{\omega_{n+1}} \qquad (n = 0, 1, 2, \ldots).$$

Note. In what follows, α, β are "constants"; γ, ξ are "variables."

Proof of Theorem. We assume (1), and we are going to construct a counter-example for the proposition $(\mathfrak{c}, \aleph_\alpha)$. Let G be the family of all dyadic functions on X, where $\bar{\bar{X}} = \aleph_\alpha$. Then $\bar{\bar{G}} = 2^{\aleph_\alpha}$, hence, by (1),

(5) $$\bar{\bar{G}} = \aleph_{\omega_\beta}.$$

Given a sequence $\{\phi_n(x)\}$ of dyadic functions on X, let F_ϕ be the family of those functions which are limits of subsequences of $\{\phi_n(x)\}$. Furthermore, let Φ be the family of *all* sequences (of dyadic functions on X), and let $\mathscr{S}$ be the system of all families F_ϕ where $\phi \in \Phi$.

It follows that

(6) $$\bar{\bar{F}}_\phi \leqslant \mathfrak{c}, \ \bar{\bar{\Phi}} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \aleph_{\omega_\beta},$$

and

(6′) $$\bar{\bar{\mathscr{S}}} \leqslant \bar{\bar{\Phi}} \quad \text{and} \quad \bar{\bar{G}} < \bar{\bar{\mathscr{S}}}.$$

(The last inequality follows from the fact that every element of G corresponds to a one-element family F_ϕ whose base converges.)

Hence, from (1), (5), (6), and (6′), we have:

(7) $$\bar{\bar{F}}_\phi < \mathfrak{c} < \aleph_{\omega_\beta}, \quad \bar{\bar{G}} = \bar{\bar{\mathscr{S}}} = \aleph_{\omega_\beta}.$$

Now, since F_ϕ is the "maximal" family with the base ϕ, every family of functions admitting a base is contained in some F_ϕ, i.e.,

(8) *If F has a base then, for some ϕ, $F \subset F_\phi \in \mathscr{S}$.*

On the assumption of (7) we are going to construct a family F° of power $< \aleph_\beta$ which is not contained in any $F_\phi \in \mathscr{S}$, which therefore, according to (8), has no base.

Let

$$F_1, F_2, \ldots F_\omega, \ldots F_\xi, \ldots |_{\omega_{\omega_\beta}}$$

be the elements of $\mathscr{S}$, ordered in a transfinite sequence.

We put

(9) $$H_\gamma = \sum_{\xi < \omega_\gamma} F_\xi \qquad (\gamma < \omega_\beta),$$

and, for each $\gamma < \omega_\beta$, let h_γ be one element of the set $G - H_\gamma$:

$$h_\gamma \in G - H_\gamma \qquad (\gamma < \omega_\beta). \tag{10}$$

This element h_γ exists because

$$\overline{\overline{H}}_\gamma < \mathfrak{c}\aleph_\gamma < \aleph_{\omega_\beta},$$

but $\overline{\overline{G}} = \aleph_{\omega_\beta}$ hence the set $G - H_\gamma$ is not empty.

Now let F° be the set of all these h_γ. Then $\overline{\overline{F}}^\circ < \aleph_\beta < \mathfrak{c}$. It follows from (10) that $h_\gamma \notin F_\xi$ for all $\xi < \omega_\gamma$. But $h_\gamma \in F^\circ$ by definition. Therefore F° cannot be contained in any F_ξ (for all $\xi < \omega_\beta$), i.e., in any $F_\phi \in \mathscr{S}$.

Thus, by (8), F° has no base, although

$$\overline{\overline{F}}^\circ < \mathfrak{c}.$$

Reference

1. F. Rothberger, *On families of real functions with a denumerable base*, Ann. Math., vol. 45 (1944), 397-406.

University of New Brunswick

AN EXTENSION OF MEYER'S THEOREM ON INDEFINITE TERNARY QUADRATIC FORMS

BURTON W. JONES

1. Introduction. Let f be a ternary quadratic form whose matrix F has integral elements with g.c.d. 1, that is, an improperly or properly primitive form according as all diagonal elements are even or not. Let d be the determinant of f (denoted by $|f|$), Ω the g.c.d. of the 2-rowed minors of F. Then $d = \Omega^2\Delta$ determines an integer Δ. Two forms f in the same genus have the same invariants Ω, Δ, d. The form whose matrix is adj F/Ω is called the *reciprocal form* of f. A theorem of Meyer, as extended by Dickson [1], who completely reworked Meyer's inadequate proof, is the following:

THEOREM 1. *If f_1 and f_2 are two properly or improperly primitive indefinite ternary quadratic forms in the same genus, they are equivalent if*

$$(\Omega, \Delta) < 2, \Omega \not\equiv 0 \pmod 4, \Delta \not\equiv 0 \pmod 4. \tag{1}$$

Meyer [3] also gave the number of classes in a genus of ternary indefinite forms in terms of sets of quadratic characters with respect to the primes common to Ω and Δ, but his proofs are obscure. Siegel recently showed the author that the forms

$$f = x_1^2 - 2x_2^2 + 64x_3^2, \quad g = (2x_1 + x_3)^2 - 2x_2^2 + 16x_3^2$$

are in the same genus but are not equivalent since the latter represents no perfect square whose factors are all congruent to 1 (mod 8). It is the purpose of this article to give a large set of genera of one class whose invariants are not relatively prime.

Let p be an odd prime factor common to Ω and Δ. It is well known [2, Theorem 25] that for k arbitrary, f is equivalent to a form

$$f_0 \equiv a_1x_1^2 + p^2a_2x_2^2 + pa_3x_3^2 \pmod{p^k}, \qquad (a_1, p) = 1. \tag{2}$$

Then the transformation K: $x_1 = py_1$, $x_2 = y_2$, $x_3 = y_3$, takes f_0 into pg where g is a form whose matrix has integral elements and

$$g \equiv pa_1y_1^2 + pa_2y_2^2 + a_3y_3^2 \pmod{p^{k-1}}.$$

We call g the *related* or *p-related* form of f and shall prove

THEOREM 2. *If a form g above is in a genus of one class, if p^3 does not divide $|g|$, and if there is an integer q, prime to p and satisfying the following conditions:*

(i) *$|q|$ is an odd prime or double an odd prime;*

(ii) *$-q$ is represented by the reciprocal form of g;*

(iii) *every solution of the congruence*

(3) $$x^2 - qy^2 \equiv 1 \pmod{p}$$

is congruent (mod p) *to a solution of the Pell equation*

(4) $$x^2 - qy^2 = 1;$$

then the form f is in a genus of one class.

Notice that (ii) imposes only congruence conditions on q and that q must be double a prime if the reciprocal of g is improperly primitive.

Theorems 1 and 2 then imply

COROLLARY 1. *There is only one class in the genus of a (properly or improperly) primitive form f if*

(i) $\Omega \not\equiv 0 \pmod 4$, $\Delta \not\equiv 0 \pmod 4$;

(ii) *for any odd prime factor p dividing both Ω and Δ, it is true that p^3 does not divide $|g|$ and there exists a q satisfying the conditions of Theorem 2.*

The conditions of Theorem 2 will be further considered in §4.

2. Equivalence of f_1 and f_2 implies that of g_1 and g_2. We consider f_1 and f_2 two primitive forms of the same genus. Then [2, Theorem 40] we may assume f_1 and f_2 congruent modulo an arbitrary power of p. Suppose $U = (u_{ij})$ is a unimodular transformation (determinant ± 1, integral elements) taking f_1 into f_2, then

$$K^{-1}UK = \begin{bmatrix} u_{11} & u_{12}p^{-1} & u_{13}p^{-1} \\ pu_{21} & u_{22} & u_{23} \\ pu_{31} & u_{32} & u_{33} \end{bmatrix},$$

which is unimodular if $u_{12} \equiv u_{13} \equiv 0 \pmod p$ and takes g_1 into g_2. Now U takes f_1 into f_2, both of the form (2), which implies:

$$a_1(u_{11}x_1 + u_{12}x_2 + u_{13}x_3)^2 + pa_2(u_{21}x_1 + u_{22}x_2 + u_{23}x_3)^2$$
$$\equiv a_1x_1^2 + pa_2x_2^2 \pmod{p^2}.$$

This implies

$$a_1u_{12}^2 \equiv a_1u_{13}^2 \equiv 0 \pmod p$$

which, since $(a_1,p) = 1$, implies $u_{12} \equiv u_{13} \equiv 0 \pmod p$ which completes our proof that $f_1 \cong f_2$ implies $g_1 \cong g_2$ where $\cong$ is the sign for equivalence. Hence the number of classes in the genus of f is not less than the number of classes in the genus of g.

3. Conditions under which $g_1 \cong g_2$ implies $f_1 \cong f_2$. As above, we may assume g_1 and g_2 congruent modulo p^k. Now let the unimodular transformation $U = (u_{ij})$ take g_1 into g_2. Then KUK^{-1} takes f_1 into f_2,

$$KUK^{-1} = \begin{bmatrix} u_{11} & pu_{12} & pu_{13} \\ u_{21}p^{-1} & u_{22} & u_{23} \\ u_{31}p^{-1} & u_{32} & u_{33} \end{bmatrix},$$

and we need $u_{21} \equiv u_{31} \equiv 0 \pmod{p}$. But

$$a_2(u_{31}x_1 + u_{32}x_2 + u_{33}x_3)^2 \equiv a_3x_3^2 \pmod{p}$$

follows from that fact that U takes g_1 into g_2 and g_1 and g_2 are both in form mod p^{k-1} given above. This implies $u_{31} \equiv u_{32} \equiv 0 \pmod{p}$ since $a_3 \equiv 0 \pmod{p}$ would imply p^2 a divisor of $|g|$ contrary to hypothesis. It remains to make $u_{21} \equiv 0 \pmod{p}$. This we do by showing that under certain circumstances we can find an automorph P of g such that the last two elements of the first column of PU are divisible by p.

Write G, the matrix of g, in the form

$$\begin{bmatrix} pB & pb_1 \\ pb_1^T & b \end{bmatrix} \equiv \begin{bmatrix} pB & 0 \\ 0 & b \end{bmatrix} \pmod{p^{k-1}}.$$

Since, under the conditions of Theorem 2, the reciprocal form of g represents $-q \pmod{p^{k-1}}$ we may take $|B| = -q$. Let the unimodular transformation U taking g_1 into g_2 be written

$$U = \begin{bmatrix} U_0 & u_1 \\ u_2 & u_{33} \end{bmatrix}$$

where $u_2 = (u_{31}, u_{32}) \equiv (0,0) \pmod{p}$. We shall first prove

LEMMA 1. *If B has an automorph A such that*
(i) $(A \mp I)B^{-1}$ *is integral for proper choice of* $\pm$,
(ii) $A \equiv U_0 \pmod{p}$,
then an integral 1×2 matrix w may be determined so that

$$P = \begin{bmatrix} A & w \\ 0 & \pm 1 \end{bmatrix},$$

and hence P^{-1} are integral automorphs of G and

$$P^{-1}U \equiv \begin{bmatrix} 1 & 0 & u_{13} \\ 0 & 1 & u_{23} \\ 0 & 0 & \pm u_{33} \end{bmatrix} \pmod{p}.$$

In order to prove this, we need to make $P^TGP = G$, that is

$$\begin{bmatrix} A^TpBA & pA^TBw \pm pA^Tb_1 \\ pw^TBA \pm pb_1^TA & pw^TBw \pm pb_1^Tw \pm pw^Tb_1 + b \end{bmatrix} = \begin{bmatrix} pB & pb_1 \\ pb_1^T & b \end{bmatrix}. \tag{5}$$

But $A^TBA = B$ and, if we can determine an integral w so that

$$A^TBw \pm A^Tb_1 = b_1, \tag{6}$$

$|P| = \pm 1$ with $|B| \neq 0$ implies that b is equal to the corresponding member in the left-hand matrix of (5). However (6) is equivalent to

$$BA^{-1}w = \mp (A^T \mp I)b_1,$$

or

$$w = \mp AB^{-1}(A^T \mp I)b_1 = \mp (I \mp A)B^{-1}b_1 = (A \mp I)B^{-1}b_1.$$

Hence w is integral if condition (i) of the Lemma holds. Furthermore, $b_1 \equiv 0 \pmod{p}$ implies $w \equiv 0 \pmod{p}$.

If, in addition, condition (ii) holds, we have

$$P^{-1} = \begin{bmatrix} A^{-1} & \mp A^{-1}w \\ 0 & \pm 1 \end{bmatrix} \equiv \begin{bmatrix} A^{-1} & 0 \\ 0 & \pm 1 \end{bmatrix} \pmod{p},$$

$$P^{-1}U \equiv \begin{bmatrix} A^{-1} & 0 \\ 0 & \pm 1 \end{bmatrix} \begin{bmatrix} U_0 & u_1 \\ 0 & u_{33} \end{bmatrix} \equiv \begin{bmatrix} I & A^{-1}u_1 \\ 0 & \pm u_{33} \end{bmatrix} \pmod{p},$$

and our proof is complete. That is, we can, under the conditions of Lemma 1, find a transformation U taking g_1 into g_2 for which $u_{21} \equiv u_{31} \equiv 0 \pmod{p}$. In other words, $g_1 \cong g_2$ implies $f_1 \cong f_2$.

It may easily be verified that

$$A = \begin{bmatrix} t - bu & -cu \\ au & t + bu \end{bmatrix} \tag{7}$$

is an automorph of $ax^2 + 2bxy + cy^2$, the form whose matrix is B, if t,u is a solution of $x^2 - qy^2 = 1$, where $-q = ac - b^2$. We prove

LEMMA 2. *Condition* (i) *of Lemma* 1 *holds if* A *is expressed in form* (7) *with* $t \equiv \pm 1 \pmod{q}$.

To prove this, note that

$$(A \mp I)B^{-1} = -q^{-1} \begin{bmatrix} c(t \mp 1) & qu - b(t \mp 1) \\ -qu - b(t \mp 1) & a(t \mp 1) \end{bmatrix},$$

which is integral if $t \equiv \pm 1 \pmod{q}$. Notice that any solution of $x^2 - qy^2 = 1$ satisfies the condition if q is an odd prime or double an odd prime.

Now, as may be shown in the same way as one establishes the automorphs of a binary form,

$$U_0^T B U_0 \equiv B \pmod{p}$$

implies, for p an odd prime,

$$U_0 \equiv \begin{bmatrix} t' - bu' & -cu' \\ au' & t' + bu' \end{bmatrix} \pmod{p},$$

where $t'^2 - qu'^2 \equiv 1 \pmod{p}$. Hence if there is a solution t,u of the Pell equation $x^2 - qy^2 = 1$ such that $t \equiv t' \pmod{p}$ we have $qu^2 \equiv qu'^2 \pmod{p}$ and thus by proper choice of sign of u' we have $A \equiv U_0 \pmod{p}$. We have proved

LEMMA 3. *If for every solution* t',u' *of the congruence* $x^2 - qy^2 \equiv 1 \pmod{p}$ *there is a solution* t,u *of the Pell equation* $x^2 - qy^2 = 1$ *such that* $t \equiv t' \pmod{p}$, *condition* (ii) *of Lemma* 1 *holds.*

These three lemmas establish Theorem 2. We now consider in more detail the conditions (ii) and (iii) of Theorem 2 and investigate the permissible values of p and q.

4. Modifications of the conditions of Theorem 2. Consider first the condition that $-q$ be represented by a ternary quadratic form h whose determinant is prime to q. We shall prove

THEOREM 3. *If h is an indefinite ternary form satisfying the conditions of Theorem* 1, *it represents $-q$ with $(q, |h|) < 2$ if and only if it represents $-q$ in $R(2)$, the ring of 2-adic integers, and in $R(r)$ for every odd prime factor of Ω, that is, if $h \equiv -q \pmod{r}$ is solvable for every such r.*

We know from Corollary 44b of [2] that if h represents $-q$ in $R(r)$ for $r = \infty$ and every prime factor, r, of $2|h|q$, there is a form h' in the genus of h which represents $-q$. But our Theorem 1 implies that h' is equivalent to h which therefore represents $-q$ if h' does. Since h is indefinite it represents $-q$ in the field of reals. It remains to show that h represents $-q$ in $R(r)$ for r an odd prime factor of $q|h|$. If $r = q$ or $\frac{1}{2}q$, Corollary 34b of [2] gives the desired result. Now for any odd prime r we may consider

$$h \equiv a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \pmod{r^2}.$$

First, if $a_1a_2 \not\equiv 0 \pmod{r}$, then

$$a_1x_1^2 + a_3x_2^2 \equiv -q \pmod{r^2}$$

solvable shows that h represents $-q$ in $R(r)$. Second, two of a_1,a_2,a_3 are divisible by r if and only if r divides Ω. Suppose $a_1 \equiv a_2 \equiv 0 \pmod{r}$. Then $h \equiv -q$ is solvable in $R(r)$ if and only if $h \equiv -q \pmod{r}$ is solvable [2, Theorem 9a]. This completes the proof.

Since g is a ternary form $\operatorname{adj}(\operatorname{adj} G) = dG$ where $d = |G|$. If Ω is the g.c.d. of the 2×2 minors of G it divides all elements of dG, and g primitive implies $d = \Omega^2\Delta$, where Δ is an integer. Furthermore, d is the g.c.d. of all elements of $\operatorname{adj}(\operatorname{adj} G)$ and hence of all 2-rowed minors of $\operatorname{adj} G$. This implies that Δ is the g.c.d. of the 2-rowed minors of the matrix of the reciprocal form of g. Hence we have

THEOREM 4. *Let p be a fixed odd prime and f a primitive form for which $\Omega \equiv \Delta \equiv 0 \pmod{p}$, neither Ω nor Δ being divisible by 4 or p^2, and g its p-related form. Then the reciprocal form of g represents $-q$ if and only if it represents it in $R(r)$ for all prime divisors r of $2\Delta/p$.*

This has the effect of imposing on $-q$ certain conditions modulo powers of 2 and mod r for odd prime factors of Δ/p.

COROLLARY. *Condition* (ii) *of Theorem* 2 *may be replaced by the conditions of Theorem* 4.

Now let us consider further the condition (iii) of Theorem 2. It may be shown that the number of solutions of the congruence (3) is

$$p - (q|p).$$

The number of solutions with $y = 0$ is 2, with $x = 0$ is $1 + (-q|p)$. Hence the number of solutions with neither x nor y zero is

$$p - (q|p) - (-q|p) - 3$$

and the number of distinct pairs of solutions x^2,y^2 with neither zero is one fourth of this number. Hence the number of distinct (mod p) pairs x^2,y^2 of solutions is

$$M = \tfrac{1}{4}\{p - (q|p) + (-q|p) + 3\}.$$

That is

$$M = \tfrac{1}{4}(p + 3) \text{ if } p \equiv 1 \pmod 4,$$

$$M = \tfrac{1}{4}(p + 1) \text{ if } p \equiv -1 \pmod 4 \text{ and } (q|p) = 1,$$

$$M = \tfrac{1}{4}(p + 5) \text{ if } p \equiv -1 \pmod 4 \text{ and } (q|p) = -1.$$

First we consider two special cases. Suppose $p = 3$ and $q \equiv 1 \pmod 3$. Then there is only one pair of solutions of the congruence, namely, $x^2 \equiv 1$, $y^2 \equiv 0 \pmod 3$, and hence condition (iii) of Theorem 2 holds. Then from Theorem 4 and Corollary 1 we prove

THEOREM 5. *An indefinite primitive ternary quadratic form f is in a genus of one class provided*

(i) (Ω,Δ) *divides* 6,
(ii) $\Omega \not\equiv 0 \not\equiv \Delta \pmod 4$,
(iii) $|f| \not\equiv 0 \pmod{81}$.

To prove this we need merely show the existence of a prime or double a prime q with $(q|3) = 1$ and satisfying the conditions of Theorem 4. This means that $q \equiv 1 \pmod 3$ and satisfies certain congruence conditions modulo powers of r where r is a prime factor of $2\Delta/3$. Dirichlet's theorem shows that such a q exists provided that these conditions are consistent and the conditions of the theorem imply that $\Delta/3$ is not divisible by 3. This completes the proof.

Furthermore, for $p = 3$, $(q|3) = 1$, condition (iii) of Theorem 2 holds even if q is negative and g a positive form. Thus we have

THEOREM 6. *For $p = 3$, a positive ternary quadratic form f is in a genus of only one class if its 3-related form g is, and if $|f| \not\equiv 0 \pmod{81}$.*

Two examples are

$$f = x^2 + 18y^2 + 3z^2, \quad g = 3x^2 + 6y^2 + z^2,$$
$$f = x^2 + 18y^2 + 6z^2, \quad g = 3x^2 + 6y^2 + 2z^2.$$

Group theoretic considerations lead to another special case of interest. Let T,U be the fundamental solution of $x^2 - qy^2 = 1$. It is well known that all solutions are given by

$$t_n + u_n\sqrt{q} = \pm (T + U\sqrt{q})^n$$

for integral powers of n. Hence under this law of combination, the solutions

(mod p) of the Pell equation form a multiplicative group H_p which must be a subgroup of the multiplicative group of solutions of the congruence (mod p). Hence s, the order of H_p, is a divisor of $2u = p - (q|p)$. Condition (iii) of Theorem 2 will be met if and only if $s = 2u$. Now s must be even since (t,u), a solution of the Pell equation, implies that $(-t,u)$ is a solution and $(0,u)$, a solution, implies that $(0,-u)$ is. Hence $s = 2s'$. But $s > 2$ unless, for the fundamental solution, $U \equiv 0 \pmod{p}$ and, with this exception, u a prime would imply $s' = u$ and $s = 2u$. Hence, *if for proper choice of sign* $\frac{1}{2}(p \pm 1)$ *is a prime, condition* (iii) of Theorem 2 holds and q *may be chosen to satisfy conditions* (i) *and* (ii) *unless* $U \equiv 0 \pmod{p}$ for the fundamental solution of the Pell equation.

To consider the general case we notice again that any solution t,u of $x^2 - qy^2 = 1$ is expressible in the form

$$t_r + u_r\sqrt{q} = \pm (T + U\sqrt{q})^r$$

where T,U is the fundamental solution. Now

$$t_r + u_r\sqrt{q} \equiv t_s + u_s\sqrt{q} \pmod{p}$$

implies

$$t_r - u_r\sqrt{q} \equiv t_s - u_s\sqrt{q} \pmod{p}$$

where if $(q|p) = -1$ by such a congruence we mean that corresponding parts are congruent and if $(q|p) = 1$ we replace $\sqrt{q}$ by a solution of $q \equiv r^2 \pmod{p}$. Hence $t_r \equiv t_s$, since p is odd and thus $u_r \equiv u_s$.

First, if $(q|p) = 1$, there are $p - 1$ solutions of the congruence and $\pm (T + U\sqrt{q})^k$ yields all solutions if and only if one of the following holds:

(a) $\omega = T + U\sqrt{q}$ is a primitive root (mod p).

(b) ω belongs to $\frac{1}{2}(p - 1)$ (mod p) and no power of ω is congruent to -1 (mod p).

We can show that condition (b) may be replaced by

(b′) ω belongs to $\frac{1}{2}(p - 1)$ (mod p) and $p \equiv 3 \pmod{4}$.

Suppose $p \equiv 1 \pmod{4}$. Then ω belonging to $\frac{1}{2}(p - 1)$ would imply $\omega^t \equiv -1 \pmod{p}$ for $t = \frac{1}{4}(p - 1)$. On the other hand, if $p \equiv 3 \pmod{4}$, $\omega^t \equiv -1 \pmod{p}$ would imply $\frac{1}{2}(p - 1)$ divides $2t$ and since the former is odd it must divide t. This would make it impossible for ω to belong to $\frac{1}{2}(p - 1)$.

Second, if $(q|p) = -1$ there are $p + 1$ solutions of the congruence and $\pm (T + U\sqrt{q})^k$ yields all solutions if and only if one of the following holds:

(a) ω belongs to $p + 1$ (mod p).

(b) ω belongs to $\frac{1}{2}(p + 1)$ (mod p) and no power of ω is congruent to -1 (mod p).

As above, we may replace condition (b) by

(b′) ω belongs to $\frac{1}{2}(p + 1)$ (mod p) and $p \equiv 1 \pmod{4}$.

5. Examples. We consider $p = 5$ and $p = 7$, giving explicit conditions for primes q or doubles of primes q satisfying condition (iii) of Theorem 2 and append a short table of values.

$$p = 5$$

Case 1. Suppose $(q|p) = 1$. The primitive roots (mod 5) are 2 and 3. Let $a^2 \equiv q \pmod 5$ and have

$$T^2 - a^2U^2 \equiv 1 \pmod 5,\ T - aU \equiv \pm 2 \pmod 5$$

imply

$$T + aU \equiv \pm 3 \pmod 5$$

and hence

$$T \equiv 0 \pmod 5$$

is the necessary and sufficient condition for (iii) of Theorem 2, since $T^2 \equiv -1 \pmod 5$ would imply $a^2U^2 \equiv -2 \pmod 5$ which is impossible.

Case 2. Suppose $(q|p) = -1$. Since $p + 1 \equiv 2 \pmod 4$ we want $\omega \not\equiv \pm 1 \pmod 5$ and $\omega^3 \equiv \pm 1 \pmod 5$. Now

$$\omega^2 = T^2 + qU^2 + 2UT\sqrt{q} \equiv 1 \pmod 5$$

only if $UT \equiv 0 \pmod 5$. But $T \equiv 0 \pmod 5$ would imply $-qU^2 \equiv 1 \pmod 5$ which would deny $(q|p) = -1$. Hence $U \equiv 0 \pmod 5$, $T \equiv \pm 1 \pmod 5$ which must be excluded. Thus the necessary and sufficient condition for (iii) is

$$T \equiv \pm 2 \pmod 5.$$

We can include both case 1 and 2 by writing

$$T \equiv 0, \pm 2 \pmod 5. \tag{8}$$

The prime and double prime values of q less than 50 for which (8) holds are:

$$3, 6, 7, 11, 14, 17, 19, 22, 31, 34, 37, 38, 43, 46, 47.$$

In terms of our general results this means that Ω and Δ may have a common factor 5 if the negative of one of the numbers in the table is represented by the reciprocal form of g.

$$p = 7$$

Case 1. Suppose $(q|p) = 1$. The primitive roots (mod 7) are 3 and 5. Here we want $\omega^3 \equiv \pm 1$ and $\omega \not\equiv \pm 1$, all congruences being (mod 7). Suppose $T + aU \equiv \pm 1$; then $T \equiv \pm 1$ which is excluded. Similarly it is easily shown that $T \equiv 0$ and $T \equiv \pm 2$ are impossible. Hence a necessary and sufficient condition for (iii) is

$$T \equiv \pm 3 \pmod 7.$$

Case 2. Suppose $(q|p) = -1$. Then ω must belong to 8 (mod 7), that is, $\omega^2 \not\equiv \pm 1$. But

$$(T + U\sqrt{q})^2 = T^2 + U^2q + 2TU\sqrt{q} \equiv \pm 1$$

imply $TU \equiv 0$. Thus $U \equiv 0$ and $T^2 \equiv 1$ or $T \equiv 0$ and $qU^2 \equiv \pm 1$ both of which are excluded. But $T^2 \equiv 9$ is impossible. We include both cases in

$$T \equiv \pm 2, \pm 3 \pmod 7. \tag{9}$$

The prime and double prime values of q less than 50 for which (9) holds are:

3, 5, 6, 10, 11, 13, 17, 19, 23, 26, 37, 38, 41, 43, 46.

Extensions of the results of this paper are being considered by the author and his students.

References

1. L. E. Dickson, *Studies in the theory of numbers* (Chicago, 1930).
2. B. W. Jones, *The arithmetic theory of quadratic forms* (Tenth Carus Monograph, Math. Assoc. Amer., 1950).
3. A. Meyer, *Über indefinite ternare quadratische Formen*, J. Reine Angew. Math., vol. 116 (1896), 317-325.